Puissance expressive des preuves circulaires

Jérôme Fortier

UNIVERSITÉ DU QUÉBEC À MONTRÉAL
DOCTORAT EN MATHÉMATIQUES
CONCENTRATION EN INFORMATIQUE MATHÉMATIQUE

AIX-MARSEILLE UNIVERSITÉ
ÉCOLE DOCTORALE 184 : MATHÉMATIQUES ET INFORMATIQUE
DOCTORAT EN INFORMATIQUE

PUISSANCE EXPRESSIVE DES PREUVES CIRCULAIRES

THÈSE EN COTUTELLE
SOUTENUE LE 19 DÉCEMBRE 2014 PAR
Jérôme FORTIER
DÉPÔT FINAL : JANVIER 2015

COMPOSITION DU JURY

M. André JOYAL,	PRÉSIDENT
M. Pieter HOFSTRA,	RAPPORTEUR
M. Paul-André MELLIÈS,	RAPPORTEUR
M. Laurent REGNIER,	MEMBRE
M. Luigi SANTOCANALE,	DIRECTEUR
M. Srečko BRLEK,	DIRECTEUR

REMERCIEMENTS

La thèse que vous vous apprêtez à lire n'est pas seulement le fruit du travail acharné d'une seule personne, mais aussi le fruit du support, de la collaboration et de l'influence de plusieurs autres, dont il importe de faire l'éloge en cette page.

Mes premiers remerciements vont, bien sûr, aux deux mentors qui ont relevé le défi de m'avoir comme étudiant lors de ce périple : messieurs Luigi Santocanale et Srečko Brlek. Luigi est à l'origine de la théorie des preuves circulaires étudiée dans toute cette thèse et sa grande collaboration à mon travail est à l'origine de ma propre compréhension de presque tout ce qui s'y rattache. Quant à Srečko, il est à l'origine de cette collaboration et de mon initiation au métier et à la vie de chercheur. Ensemble, ils m'ont enseigné ce qu'était l'informatique théorique.

Cette thèse doit aussi beaucoup à l'influence des discussions avec plusieurs autres collaborateurs rencontrés dans l'une des deux institutions où j'ai travaillé, l'Université du Québec à Montréal et Aix-Marseille Université, ou encore dans des conférences et ateliers auxquels j'ai eu le plaisir d'assister. J'ai aussi une pensée spéciale pour les membres du jury de cette thèse, messieurs André Joyal, Laurent Regnier, Paul-André Melliès et Pieter Hofstra, pour avoir accepté de l'évaluer et d'y contribuer par leur expertise et leurs questions.

Bien sûr, rien de cela n'aurait été possible sans mes généreux commanditaires : le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG), Campus France, l'Institut des Sciences Mathématiques (ISM), le Fonds de recherche du Québec - Nature et technologies (FRQNT) ainsi que le Laboratoire de

combinatoire et d'informatique mathématique (LaCIM) à Montréal et le Laboratoire d'Informatique Fondamentale (LIF) à Marseille.

Enfin, j'aimerais remercier celles et ceux qui ont fait partie de ma vie, de façon épisodique ou continue, au cours de ces années de doctorat. Vous avez fait de cette aventure une expérience humaine inoubliable.

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

RÉSUMÉ

Cette recherche vise à établir les propriétés fondamentales d'un système formel aux preuves circulaires introduit par Santocanale, auquel on a rajouté la règle de coupure. On démontre, dans un premier temps, qu'il y a une pleine correspondance entre les preuves circulaires et les flèches issues des catégories dites μ-bicomplètes. Ces flèches sont celles que l'on peut définir purement à partir des outils suivants : les produits et coproduits finis, les algèbres initiales et les coalgèbres finales. Dans la catégorie des ensembles, les preuves circulaires dénotent donc les fonctions qu'on peut définir en utilisant les produits cartésiens finis, les unions disjointes finies, l'induction et la coinduction. On décrit également une procédure d'élimination des coupures qui produit, à partir d'une preuve circulaire finie, une preuve sans cycles et sans coupures, mais possiblement infinie. On démontre que l'élimination des coupures fournit une sémantique opérationnelle aux preuves circulaires, c'est-à-dire qu'elle permet de calculer les fonctions dénotées par celles-ci, par le moyen d'une sorte d'automate avec mémoire. Enfin, on s'intéresse au problème de la puissance expressive de cet éliminateur de coupures, c'est-à-dire à la question de caractériser la classe des expressions qu'il peut calculer. On démontre, par une simulation, que l'éliminateur des coupures est strictement plus expressif que les automates à pile d'ordre supérieur.

MOTS-CLÉS : preuves circulaires, logique catégorique, catégories μ-bicomplètes, points fixes, algèbres initiales, coalgèbres finales, élimination des coupures, automates à pile d'ordre supérieur

KEYWORDS : circular proofs, categorical logic, μ-bicomplete categories, fixpoints, initial algebras, final coalgebras, cut-elimination, higher-order pushdown automata

INTRODUCTION

La déduction est, depuis Euclide, l'instrument de validation par excellence des mathématiciens. Si un énoncé mathématique se déduit logiquement à partir d'autres énoncés considérés comme étant vrais, alors il est lui-même considéré vrai. Bien que la validité de ce principe soit difficilement discutable — pourvu qu'on s'entende sur les raisonnements logiques admissibles, ce qui n'est pas une mince affaire — on peut toutefois s'interroger sur sa réciproque : pour qu'un énoncé soit considéré vrai, doit-il *absolument* être obtenu par un raisonnement logique basé sur d'autres énoncés déjà considérés vrais ?

La réponse est évidemment négative : il faut d'abord accepter certains énoncés sans démonstration (les axiomes), afin de fonder la déduction quelque part. À cette exception près, la plupart des mathématiciens (encore aujourd'hui), influencés par l'ouvrage fondamental *Principia mathematica* de Whitehead et Russell (1913), considèrent la déduction comme étant la *seule* garantie de validité des énoncés mathématiques. Une conséquence immédiate de cela est qu'on doit bannir les raisonnements circulaires : ceux-ci concernent, en effet, des énoncés déduits à partir d'eux mêmes, donc devant être considérés vrais avant d'être considérés vrais, ce qui n'est pas chronologiquement possible. Bien sûr, les logiciens savent depuis Gödel (1931) que *Principia mathematica* et les systèmes logiques de même nature ne peuvent pas caractériser la vérité mathématique, notamment parce qu'ils ne peuvent pas, à moins d'être incohérents, démontrer leur propre cohérence, pour des raisons liées à l'auto-référence. Mais l'incomplétude d'un tel système apparaît être un moindre mal face au risque d'incohérence encouru en permettant les preuves circulaires.

Or, l'entreprise même de la logique mathématique, soit de raisonner mathématiquement sur le raisonnement mathématique, n'est-elle pas circulaire ? *Principia mathematica* répond à ce paradoxe en introduisant la notion de méta-langage, ou méta-formalisme. Pour pouvoir raisonner formellement sur un formalisme donné (une logique symbolique), il faut se trouver à l'extérieur de ce formalisme, donc dans un méta-formalisme. Mais comment formaliser ce méta-formalisme ? Pour le faire, il suffit de se placer dans un méta-méta-formalisme, et ainsi de suite. On obtient ainsi, par une sorte de récurrence, une chaîne infinie de formalismes.

Le traitement qui est fait des formalismes logiques dans *Principia mathematica* est donc, essentiellement, le même qu'il y est fait de la théorie des ensembles. L'idée de la théorie des types de Russell (1908), reprise sous le nom d'*axiome de fondation* dans la théorie des ensembles de Zermelo-Fraenkel (qui constitue encore la pensée dominante sur le sujet), impose aux ensembles d'être *bien fondés*, c'est-à-dire construits à partir d'ensembles plus élémentaires (de *type inférieur*), le plus élémentaire de tous étant l'ensemble vide. Cela permet, encore une fois, d'évacuer la circularité et de disqualifier les paradoxes connus jadis de la théorie naïve des ensembles, tels le paradoxe de Cantor (sur l'ensemble de tous les ensembles) et celui de Russell, concernant l'ensemble R de tous les ensembles qui ne sont pas un élément d'eux-mêmes (on a donc $R \in R$ si et seulement si $R \notin R$).

On peut toutefois se demander si une telle hiérarchisation des formalismes est appropriée pour la logique. Il s'agit, en effet, d'un chemin bien complexe pour justifier le formalisme initial qui se voulait être une modélisation logico-mathématique de notre propre activité logico-mathématique. Pire encore : tenter de justifier le niveau de base en présupposant toujours l'existence d'un niveau plus complexe est tout le contraire de l'idée de tout ramener à des axiomes, idée qui a emmené à vouloir bannir l'auto-référence en premier lieu.

Quelques questions de nature méta-mathématique qui surgissent de ces remarques sont les suivantes. Y a-t-il lieu de faire une certaine place aux raisonnements circulaires dans la logique mathématique ? Peut-on y gagner quelque chose d'appréciable (en esthétique ou en efficacité) ? Comment distinguer les preuves circulaires paradoxales de celles qui ne le sont pas ? Comment interpréter ces dernières ? L'état de la recherche sur ces questions est encore trop embryonnaire pour apporter une réponse définitive à ces questions, mais mentionnons par exemple les travaux de Brotherston et Simpson (2011) qui proposent une modélisation de la méthode de démonstration *par descente infinie* de Fermat via une logique aux preuves circulaires.

Notre approche est différente et explore plutôt les preuves sous l'angle de la calculabilité. Quelles entités mathématiques peut-on exprimer, voire calculer, par des formalismes circulaires ? Les liens entre logique et calculabilité sont, bien sûr, intrinsèques et remontent aux fondements même de l'informatique avec la thèse de Church–Turing. On s'inspire, en particulier, du paradigme de la programmation fonctionnelle, notamment du langage Haskell, qui permet de définir des structures de données de façon circulaire. Par exemple, le type `Liste t` des listes d'éléments de type `t` peut être implémenté par la commande suivante :

```
data Liste t = Nil | Cons t (Liste t).
```

Dans cette instruction, `Nil` et `Cons` sont ce qu'on appelle des *constructeurs de type*. Ce sont deux fonctions,

$$\texttt{Nil} : \mathbf{1} \to \texttt{Liste t} \quad \text{et} \quad \texttt{Cons} : \texttt{t} \times \texttt{Liste t} \to \texttt{Liste t}$$

(où $\mathbf{1}$ est un singleton, c'est-à-dire que `Nil` ne prend aucun argument), qui déterminent toutes les possibilités pour un élément $\ell \in \texttt{Liste t}$. On peut interpréter ces possibilités comme suit : soit ℓ est la liste vide, ou sinon, ℓ est une liste construite à partir d'un symbole $a \in \texttt{t}$ (la tête de la liste ℓ) et d'une autre liste $\ell' \in \texttt{Liste t}$ (la

queue de ℓ). On obtient donc une définition des listes par l'équation ensembliste suivante :

$$\texttt{Liste t} := \mathbf{1} + (\texttt{t} \times \texttt{Liste t}),$$

où + dénote l'union disjointe (le *coproduit*). Une telle définition de `Liste t` est toutefois *formellement interdite* par l'axiome de fondation. Une solution, proposée par Aczel (1988) et plus largement développée par Barwise et Moss (1996), est de rejeter l'axiome de fondation pour le remplacer par un axiome plus permissif (dit d'anti-fondation). On obtient alors la théorie des ensembles *anti-fondés*, qui est équiconsistante à la théorie des ensembles classique, tout en étant plus générale : on peut y définir, par exemple, l'ensemble $\Omega := \{\Omega\}$ qui n'a pas d'équivalent classique, mais n'est pas paradoxal en soi.

Le développement de cette nouvelle théorie des ensembles et de la programmation fonctionnelle en général n'aurait sans doute pas été envisageable sans la contribution de la théorie des catégories qui, depuis son invention par Eilenberg et MacLane (1945), se substitue, de façon de plus en plus incontournable, à la théorie des ensembles en tant que doctrine des fondements des mathématiques (voir Lambek et Scott, 1988). Les travaux de Lawvere (1969) résolvent d'ailleurs les paradoxes de Cantor et de Russell ainsi que le théorème d'incomplétude de Gödel, en tant que simple théorèmes de points fixes dans la catégorie des ensembles (voir aussi Yanofsky, 2003).

Les outils catégoriques qui justifient la théorie des ensembles anti-fondés et une part de la programmation fonctionnelle sont les *algèbres initiales* et les *coalgèbres finales*, dont une bonne introduction se trouve dans (Jacobs et Rutten, 1997). Essentiellement, les algèbres initiales servent, dans la catégorie des ensembles, à définir des fonctions *par induction* (sur les nombres naturels, sur les mots ou les arbres finis, sur les termes d'une grammaire, etc.). Les objets sur lesquels on peut appliquer l'induction ont la particularité d'être définis par des constructeurs de

type (comme `Nil` et `Cons` ci-haut) sur lesquels on peut faire une récurrence. Quant aux coalgèbres finales, leur rôle est de permettre les définitions *par coinduction*, par exemple de mots et d'arbres infinis, de langages, etc. Les objets coinductifs se définissent non pas à partir de constructeurs mais de *destructeurs* (mieux connus sous le nom de *fonctions de transitions*) : on doit décrire l'observation qui résulte d'un changement d'état de ces objets (par un automate ou des règles de réécriture, par exemple).

Les algèbres initiales et les coalgèbres finales sont des outils mathématiques bien établis de nos jours. Mais ils sont souvent vus en opposition l'un de l'autre : peu de travaux s'efforcent de les étudier ensemble, comme faisant partie d'une seule et même entité. À cette fin, la Partie I de la thèse que vous vous apprêtez à lire, en plus d'établir au Chapitre 1 les notations et quelques faits sur les structures discrètes qui nous intéressent (mots, arbres et graphes), dresse au Chapitre 2 un portrait sommaire de la théorie des algèbres initiales et des coalgèbres finales, pour aboutir au concept de *système dirigé d'équations*. Ces systèmes d'équations particuliers permettent de définir des structures de données entrelaçant induction et coinduction.

Les algèbres initiales et les coalgèbres finales sont, respectivement, des généralisations des notions de plus petit et plus grand point fixe, issues du μ-calcul propositionnel (Pratt, 1981; Kozen, 1983). En annexe de sa thèse, Santocanale (2000) introduit un système logique pour faire des démonstrations en μ-calcul propositionnel, plus détaillé et adapté aux catégories dans (Santocanale, 2001, 2002a,b). La particularité de ce formalisme est qu'*il permet des preuves circulaires*, pourvu que les cycles de celles-ci satisfassent une certaine propriété (la condition de garde) qui en assure la validité. En effet, ces preuves circulaires peuvent être interprétées comme des programmes dont les structures de données sont encodées par des systèmes dirigés d'équations. De façon plus abstraite, elles dénotent des flèches de

la catégorie μ-bicomplète libre (Santocanale, 2002b). L'ennui est que le système n'est pas *plein* : on peut trouver des flèches de la catégorie μ-bicomplète libre qui ne sont pas représentables par une preuve circulaire.

La Partie II de la présente thèse est dédiée à la réparation de cette lacune du système de Santocanale. Dans le Chapitre 3, on redéfinit les preuves circulaires, mais en rajoutant au système la règle de coupure, qui était absente dans les précédents travaux de Santocanale. La présentation informelle qui en est faite est axée sur une interprétation des preuves en tant que programmes. On adapte alors la condition de garde en conséquence, de façon à préserver l'adéquation du système, qu'on démontrera au Chapitre 4. On verra aussi, dans ce chapitre, que ce nouveau système a la propriété de plénitude recherchée. Le Chapitre 5 est dédié à la description d'un algorithme d'élimination des coupures. L'algorithme fonctionne comme une sorte d'automate avec mémoire, qui construit un arbre de preuve, sans occurrences de la règle de coupure et possiblement infini, à partir d'une preuve circulaire donnée. La preuve de la productivité de cet algorithme n'étant pas triviale, la majeure partie du chapitre y est dédiée. Enfin, le Chapitre 6 concerne le lien entre les deux sémantiques des preuves circulaires : leur sémantique dénotationnelle (en tant que flèches de certaines catégories abstraites) et leur sémantique opérationnelle (en tant que programmes qui calculent des fonctions). L'élimination des coupures est au coeur de cette correspondance, puisqu'elle est le processus d'exécution des preuves circulaires (en tant que programmes).

Enfin, la Partie III concerne le problème d'évaluer la puissance expressive des preuves circulaires. La question est donc la suivante : quelles sont les fonctions que l'on peut dénoter par des preuves circulaires et calculer grâce à l'éliminateur de coupures ? On démontre, au Chapitre 7, que les arbres d'ordre supérieur sont calculables dans ce contexte. Les arbres en question sont ceux qui sont acceptés par des automates d'ordre supérieur, c'est-à-dire des automates qui peuvent manipuler

des piles de piles de... de piles (Knapik *et al.*, 2002; Caucal, 2003). Cela signifie que l'éliminateur de coupures, en tant que machine abstraite, possède au moins la puissance de calcul de ces automates. On verra aussi que la réciproque n'est pas vraie, c'est-à-dire que l'éliminateur de coupures est strictement plus expressif que les automates d'ordre supérieur, sans toutefois parvenir à caractériser cette puissance.

Première partie

Préliminaires

CHAPITRE I

QUELQUES STRUCTURES ORDONNÉES

Ce chapitre, dont la démarche est assez détachée du reste de cet ouvrage, vise deux objectifs. Le premier, qui justifie de placer ce chapitre au début de la thèse, est d'établir la notation qui sera utilisée plus tard, quand il sera question d'outils discrets tels que les mots, les arbres, les langages et les graphes. On en profitera également pour définir quelques relations d'ordre relatives à ces structures. Les propriétés, parfois techniques, de ces relations d'ordre seront fondamentales à certaines des démonstrations des Chapitres 4, 5 et 6, mais leurs preuves se situant hors du contexte des chapitres en question, il convient de s'en débarrasser dès maintenant. C'est le second objectif du présent chapitre.

1.1 Mots

Soit A un ensemble non vide, usuellement appelé ***alphabet***. L'ensemble des ***mots finis*** sur A, dénoté A^* est le plus petit ensemble qui comprend un élément dénoté ε (le mot vide) et tel que pour tout $a \in A$ et $u \in A^*$, l'expression $(a{:}u)$ appartient à A^*. En d'autres termes, A^* est le monoïde libre engendré par A, où l'opération du monoïde (la ***concaténation***) est définie récursivement par $\varepsilon \cdot v = v$ et $(a{:}u) \cdot v = a{:}(u \cdot v)$. De façon similaire, la *longueur* d'un mot $u \in A^*$ est un nombre naturel défini comme suit : $|\varepsilon| = 0$ et $|a{:}u| = 1 + |u|$. Par abus de langage,

on considérera les éléments de A comme des mots de longueur 1, via l'injection $a \mapsto (a{:}\varepsilon) : A \to A^*$. La concaténation n'est donc qu'une extension du constructeur $'{:}'$ et, sans ambiguïté, on se permettra d'écrire uv au lieu de $u \cdot v$ pour la dénoter.

Soit A^ω l'ensemble des ***mots infinis*** sur A (indicés par $\mathbb{N}$). Une façon simple de le définir est de dire qu'il s'agit de l'ensemble de toutes les fonctions $u : \mathbb{N} \to A$. Notons que, tout comme pour les mots non vides, une telle fonction u peut être associée, de façon unique, à l'expression $a \cdot u'$, où $a = u(0)$ s'appelle la ***tête*** de u (dénotée $\texttt{Head}(u)$) et $u' : \mathbb{N} \to A$ est la fonction (appelée ***queue*** de u et dénotée $\texttt{Tail}(u)$) définie par l'équation $u'(x) = u(x+1)$. On se permettra donc, à plusieurs occasions, de traiter les mots infinis de la même manière que leurs homologues finis, c'est-à-dire sans explicitement les traiter comme des fonctions.

Soit $A^\infty = A^* \cup A^\omega$. On peut étendre partiellement l'opération de concaténation à A^∞. En effet, dans le cas où $u \in A^*$ et $v \in A^\infty$, on peut définir $u \cdot v$ en utilisant la même définition que dans le cas de A^*. Dans le cas $u \in A^\omega$, on définit $u \cdot \varepsilon = u$, mais on ne peut définir $u \cdot v$ pour v quelconque. Par ailleurs, on peut étendre la définition de longueur, en posant $|u| = \infty$ si $u \in A^\omega$. Un ***langage*** sur A est un sous-ensemble quelconque de A^∞.

1.2 Relations d'ordre sur les mots

L'***ordre préfixe*** est la relation sur A^∞ définie par $u \sqsubseteq v$ (lire : *u est un préfixe de v*) si et seulement s'il existe $w \in A^\infty$ tel que $v = u \cdot w$. On écrira $u \sqsubset v$ pour signifier $u \sqsubseteq v$ et $u \neq v$.

Proposition 1.1. *La relation $\sqsubseteq$ est une relation d'ordre sur A^∞.*

Démonstration.

– *Réflexivité.* Soit $u \in A^\infty$. Puisque $u = u \cdot \varepsilon$, alors $u \sqsubseteq u$.
– *Transitivité.* Soit $u \sqsubseteq v \sqsubseteq w$. Alors il existe $x, y \in A^\infty$ tel que $v = u \cdot x$ et $w = v \cdot y$. Alors $w = (u \cdot x) \cdot y = u \cdot (x \cdot y)$, donc $u \sqsubseteq w$.
– *Antisymétrie.* Soit $u \sqsubseteq v \sqsubseteq u$. Alors il existe $x, y \in A^\infty$ tels que $v = u \cdot x$ et $u = v \cdot y$. Si $x = y = \varepsilon$, on en conclut immédiatement que $u = v$ comme voulu. Supposons donc le contraire : sans perte de généralité, $x \neq \varepsilon$. On a donc $|v| = |u \cdot x| > |u| = |v \cdot y| \geq |v|$, une contradiction. □

Notons qu'il n'y a pas de raison de supposer, étant donné deux mots $u, v \in A^\infty$, que l'un soit un préfixe de l'autre. Le lemme suivant donne un critère utile qui assure la comparabilité.

Lemme 1.2. *Soit $u, v \in A^\infty$, et supposons qu'il existe $w \in A^\infty$ tel que $u \sqsubseteq w$ et $v \sqsubseteq w$. Alors, ou bien $u \sqsubseteq v$, ou bien $v \sqsubseteq u$.*

Démonstration. Soit $x, y \in A^\infty$ tels que $u \cdot x = w = v \cdot y$. Si $x = \varepsilon$, alors $u = w$ et donc, $v \sqsubseteq u$. Sinon, puisque la concaténation $u \cdot x$ est définie, on a forcément $u \in A^*$. Dans ce cas, on procède par récurrence sur u.

Si $u = \varepsilon$, alors on a immédiatement $u \sqsubseteq v$, puisque $v = \varepsilon \cdot v$. De même, si $v = \varepsilon$, on conclut $v \sqsubseteq u$. Sinon, on peut écrire $u = au'$ et $v = bv'$ pour certains $a, b \in A$. Donc $w = u \cdot x = (au') \cdot x = a(u' \cdot x)$ et de la même manière, $w = b(v' \cdot y)$. Par unicité, on déduit $a = b$ et $u' \cdot x = w' = v' \cdot y$. Donc $u' \sqsubseteq w'$ et $v' \sqsubseteq w'$. Par hypothèse de récurrence, on sait alors que $u' \sqsubseteq v'$ ou bien $v' \sqsubseteq u'$.

Si $u' \sqsubseteq v'$, il existe alors $z \in A^\infty$ tel que $v' = u' \cdot z$. On a donc $u \sqsubseteq v$, puisque $v = av' = a(u' \cdot z) = (au') \cdot z = u \cdot z$. De la même façon, si $v' \sqsubseteq u'$, on peut conclure que $v \sqsubseteq u$. □

Lemme 1.3. *Pour $n \leq |v|$, il existe un unique préfixe $u \sqsubseteq v$ de longueur n. On le dénotera $v_{\restriction n}$.*

Démonstration. On procède par induction sur n. Si $n = 0$, il suffit de prendre $u = \varepsilon$ (c'est le seul mot de longueur 0). Sinon $|v| > 0$, donc on peut écrire $v = av'$ pour $a \in A$. Par hypothèse d'induction, il existe un unique $w \sqsubseteq v'$ de longueur $(n-1)$. Il suffit alors de prendre $u = aw$. □

Étant donné une chaîne dénombrable $u_0 \sqsubseteq u_1 \sqsubseteq u_2 \sqsubseteq \ldots \in A^\infty$, sa ***limite*** $\bigsqcup_{n\in\mathbb{N}} u_n \in A^\infty$ est définie comme suit. S'il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, $u_n = u_{n_0}$, alors on pose $\bigsqcup_{n\in\mathbb{N}} u_n := u_{n_0}$. Sinon, on peut trouver un unique $v \in A^\omega$ tel que pour tout n, $u_n \sqsubset v$. On définit alors $\bigsqcup_{n\in\mathbb{N}} u_n := v$. Notons que la limite d'une chaîne est la plus petite borne supérieure de celle-ci.

Une autre relation d'ordre qu'on va considérer sur A^∞ est l'***ordre purement alphabétique***. On suppose que l'alphabet A est lui-même doté d'une relation d'ordre total $\leq$. Alors on écrit $u \prec v$ si et seulement s'il existe $w \in A^*$ et $a, b \in A$ tels que $a < b$, $w \cdot a \sqsubseteq u$ et $w \cdot b \sqsubseteq v$. Le mot w dans cette définition est le *plus grand commun préfixe* de u et de v, qu'on dénotera $u \sqcap v$. Naturellement, on écrira $u \preceq v$ pour signifier $u \prec v$ ou $u = v$.

Proposition 1.4. *La relation $\preceq$ est une relation d'ordre sur A^∞.*

Démonstration.

- *Réflexivité.* Puisque $u = u$, alors $u \preceq u$ par définition.
- *Transitivité.* Soit $u \preceq v \preceq w$. Si $u = v$ ou $v = w$, il n'y a rien à démontrer. Sinon, on a $u \prec v \prec w$. Soit alors $p = u \sqcap v$, $q = v \sqcap w$, et soit $a, b, c, d \in A$ tels que $a < b$, $c < d$, $p \cdot a \sqsubseteq u$, $p \cdot b \sqsubseteq v$, $q \cdot c \sqsubseteq v$ et $q \cdot d \sqsubseteq w$. Alors $p \sqsubseteq v$ et $q \sqsubseteq v$. Par le Lemme 1.2, ou bien $p \sqsubseteq q$, ou bien $q \sqsubseteq p$. On traite alors trois cas :

  1. Si $p = q$, par unicité du préfixe de longueur $(|p| + 1)$ de v (Lemme 1.3), on a donc $p \cdot b = p \cdot c$, d'où on déduit $b = c$ et donc $a < d$. Or, puisque $p \cdot a \sqsubseteq u$ et $p \cdot d \sqsubseteq w$, on a bien $u \prec w$.

2. Si $p \sqsubset q$, alors puisque $p \cdot b \sqsubseteq v$, $q \sqsubseteq v$ et $|p \cdot b| \leq |q|$, avec le Lemme 1.2 on conclut $p \cdot b \sqsubseteq q$. Donc $p \cdot b \sqsubseteq w$ par transitivité de $\sqsubseteq$, d'où on peut conclure $u \prec w$ (parce que $a < b$).
3. Si $q \sqsubset p$, alors de façon similaire, on obtient $q \cdot c \sqsubseteq p \sqsubseteq u$ d'où on conclut $u \prec w$ (parce que $c < d$).

– *Antisymétrie.* Soit $u \preceq v \preceq u$ et supposons qu'on ait $u \neq v$ (donc $u \prec v \prec u$). Soit $w = u \sqcap v = v \sqcap u$, et soit $a, b, c, d \in A$ tels que $a < b$, $c < d$, $w \cdot a \sqsubseteq u$, $w \cdot b \sqsubseteq v$, $w \cdot c \sqsubseteq v$ et $w \cdot d \sqsubseteq u$. À l'aide du Lemme 1.3, on obtient donc $a = d$ et $b = c$. Donc $a < b = c < d = a$, une contradiction. □

Aucun des deux ordres $\sqsubseteq$ et $\preceq$ sur A^∞ n'est total. Toutefois, en les combinant, on obtient l'***ordre lexicographique***

$$u \leq_{\text{lex}} v \qquad \Longleftrightarrow \qquad u \sqsubseteq v \text{ ou } u \preceq v.$$

Proposition 1.5. *La relation $\leq_{\text{lex}}$ est une relation d'ordre total sur A^∞.*

Démonstration.

– *Réflexivité.* Découle directement de la réflexivité de $\sqsubseteq$ et de $\preceq$.

– *Transitivité.* Soit $u \leq_{\text{lex}} v \leq_{\text{lex}} w$. Seuls deux cas ne sont pas déjà traités :

1. Si $u \prec v$ et $v \sqsubseteq w$, soit $x = v \sqcap w$ et $a, b \in A$ tels que $a < b$, $x \cdot a \sqsubseteq u$ et $x \cdot b \sqsubseteq v$. Par transitivité de $\sqsubseteq$, on a également $x \cdot b \sqsubseteq w$, donc $u \prec w$.
2. Si $u \sqsubseteq v$ et $v \prec w$, $x = v \sqcap w$ et $a, b \in A$ tels que $a < b$, $x \cdot a \sqsubseteq v$ et $x \cdot b \sqsubseteq w$. Par le Lemme 1.2, on a soit $x \cdot a \sqsubseteq u$, ou bien $u \sqsubset x \cdot a$. Dans le premier cas, on trouve immédiatement $u \prec w$ et dans le second, on obtient $u \sqsubseteq x \sqsubset w$. Donc $u \leq_{\text{lex}} w$ dans tous les cas.

– *Antisymétrie.* Soit $u \leq_{\text{lex}} v \leq_{\text{lex}} u$. Sans perte de généralité, le seul cas qui n'est pas déjà traité est le cas $u \sqsubset v$ et $v \prec u$. Or, ce cas est impossible, puisque si $u \sqsubset v$, alors $u \sqcap v = u$, et il n'y a pas de $a \in A$ tel que $u \cdot a \sqsubseteq u$.

– *Totalité.* Soit $u, v \in A^\infty$, et soit $w = u \sqcap v$. Si $w = u$, alors $u \sqsubseteq v$. De même, si $w = v$, alors $v \sqsubseteq u$. Sinon, il existe $a, b \in A$ tels que $a \neq b$, $w \cdot a \sqsubseteq u$ et $w \cdot b \sqsubseteq v$. Or, par hypothèse, l'ordre $\leq$ est total sur A. On a donc soit $a < b$ (auquel cas $u \prec v$), soit $b < a$ (auquel cas $v \prec u$). □

1.3 Branches d'un langage

Un langage $L \subseteq A^\infty$ est ***ω-préfixe-complet*** si, pour toute chaîne dénombrable $u_0 \sqsubseteq u_1 \sqsubseteq u_2 \sqsubseteq \ldots \in L$, on a $\bigsqcup_{n\in\mathbb{N}} u_n \in L$. Soit $\overline{L} \subseteq A^\infty$ le plus petit langage ω-préfixe-complet qui contient L. Une ***branche*** de L est un mot $\beta \in \overline{L}$ tel que pour tout $u \in \overline{L}$, si $\beta \sqsubseteq u$, alors $\beta = u$. Soit ∂L l'ensemble des branches de L. On dit qu'une branche β est *infinie* si $|\beta| = \infty$, et qu'elle est *finie* sinon. Le but de cette section est d'étudier l'ordre lexicographique restreint à ∂L.

Lemme 1.6. *Soit $\beta, \gamma \in \partial L$. Alors $\beta \preceq \gamma$ si et seulement si $\beta \leq_{\text{lex}} \gamma$. En particulier, l'ordre $\preceq$ est total sur ∂L.*

Démonstration. Par définition, si $\beta \preceq \gamma$, alors $\beta \leq_{\text{lex}} \gamma$. Réciproquement, si $\beta \sqsubseteq \gamma$, alors parce que β est une branche, on a $\beta = \gamma$ et donc $\beta \preceq \gamma$. □

Un langage $L \subseteq A^\infty$ est ***préfixe-clos*** si pour tout $v \in L$ et $u \in A^\infty$, $u \sqsubseteq v \in L$ implique $u \in L$. Le Lemme suivant indique qu'on peut supposer cette propriété sans perte de généralité pour étudier ∂L. Soit $\downarrow L$ le plus petit langage préfixe-clos qui contient L.

Lemme 1.7. *Soit $L \subseteq A^\infty$. Alors $\downarrow(\overline{L}) = \overline{(\downarrow L)}$ et $\partial L = \partial(\overline{L}) = \partial(\downarrow L)$.*

Démonstration. Puisque $L \subseteq \downarrow L$, alors par minimalité, $\overline{L} \subseteq \overline{\downarrow L}$. Or, $\overline{\downarrow L}$ est préfixe-clos, donc par minimalité, $\downarrow(\overline{L}) \subseteq \overline{(\downarrow L)}$. Réciproquement, puisque $L \subseteq \overline{L}$,

alors $\downarrow L \subseteq \downarrow(\overline{L})$. Mais $\downarrow(\overline{L})$ est lui-même ω-préfixe-complet, donc par minimalité, on a $\overline{(\downarrow L)} \subseteq \downarrow(\overline{L})$.

Ensuite, l'égalité $\partial L = \partial(\overline{L})$ découle directement de la définition de branche, puisque clairement, $\overline{\overline{L}} = \overline{L}$.

Soit $\beta \in \partial L$. Donc $\beta \in \overline{L} \subseteq \overline{\downarrow L}$. Soit $u \in \overline{(\downarrow L)}$ tel que $\beta \sqsubseteq u$. Puisque $\overline{(\downarrow L)} = \downarrow(\overline{L})$, il existe $v \in (\overline{L})$ tel que $u \sqsubseteq v$. Donc $\beta \sqsubseteq v$ et puisque $\beta \in \partial L$, on peut conclure $\beta = v$. Donc $u \sqsubseteq \beta$ d'où on conclut $\beta = u$. Ainsi, $\beta \in \partial(\downarrow L)$ et on a montré l'inclusion $\partial L \subseteq \partial(\downarrow L)$.

Réciproquement, soit $\beta \in \partial(\downarrow L)$. En particulier, $\beta \in \overline{(\downarrow L)} = \downarrow(\overline{L})$ et donc, il existe $\gamma \in \overline{L}$ tel que $\beta \sqsubseteq \gamma$. Or, $\overline{L} \subseteq \downarrow(\overline{L}) = \overline{(\downarrow L)}$, donc $\gamma \in \overline{(\downarrow L)}$. Puisque β est une branche, on conclut $\beta = \gamma$. Ainsi, $\beta \in \overline{L}$. Maintenant, soit $u \in \overline{L}$ tel que $\beta \sqsubseteq u$. Alors encore une fois, $u \in \overline{(\downarrow L)}$ et donc $u = \beta$. Par conséquent, $\beta \in \partial L$ et cela détermine l'inclusion $\partial(\downarrow L) \subseteq \partial L$. □

On dit que L est ***à branchements finis*** si, pour tout $u \in L$, il y a seulement un nombre fini de $a \in A$ tels que $u \cdot a \in L$. C'est, par exemple, le cas lorsque A est un alphabet fini. Possiblement le résultat le plus connu sur les langages à branchements finis est le Lemme de Kőnig (1936), dont voici une version un peu renforcée (car elle fait intervenir l'ordre lexicographique).

Lemme 1.8 (Kőnig, 1936)**.** *Soit L un langage à branchements finis, qui contient une infinité de mots. Alors L admet une branche infinie minimale ainsi qu'une branche infinie maximale (par rapport à l'ordre lexicographique).*

Démonstration. Voici une construction de la branche infinie maximale, la branche minimale étant construite de la même façon après avoir interverti l'ordre sur A. Par le Lemme 1.7, on peut supposer que le langage L est préfixe-clos. Pour tout

$u \in A^*$, soit $L/u = \{v \in L : u \sqsubseteq v\}$.

Soit $u_0 = \varepsilon$. Puisque L est non vide et préfixe-clos, alors $u_0 \in L$. De plus, on a $L/u_0 = L$, qui est infini par hypothèse.

Maintenant, supposons qu'on a défini $u_n \in L$ de sorte que L/u_n soit infini. Puisque L est à branchements finis, alors l'ensemble

$$X_n = \{a \in A : L/(u_n \cdot a) \text{ est infini}\}$$

est fini et, puisque L/u_n est infini, le principe des nids de pigeons implique $X_n \neq \varnothing$. Soit donc $\overline{a} = \max(X_n)$ et $u_{n+1} = u_n \cdot \overline{a}$. Par construction, L/u_{n+1} est encore infini et, en particulier, puisque L est préfixe-clos, on a $u_{n+1} \in L$.

On construit ainsi une chaîne dénombrable $u_0 \sqsubset u_1 \sqsubset u_2 \sqsubset \cdots \in L$. Soit $\beta = \bigsqcup_{n\in\mathbb{N}} u_n$. Par construction, β est une branche infinie de L. Il reste à montrer qu'elle est maximale.

Supposons donc qu'il existe une branche infinie γ telle que $\beta \prec \gamma$. Soit $w = \beta \sqcap \gamma$ et $n = |w|$. Alors par construction, $w = u_n$. Or, puisque $\beta \prec \gamma$, il existe $a, b \in A$ tels que $a < b$, $u_n \cdot a \sqsubseteq \beta$ et $u_n \cdot b \sqsubseteq \gamma$. Mais alors, $u_n \cdot a = u_{n+1}$ et par construction, $a = \max(X_n)$. Or, puisque γ est une branche infinie, $L/(u_n \cdot b)$ doit être infini, c'est-à-dire $b \in X_n$, et puisque $a < b$, on rencontre une contradiction. □

Non seulement l'énoncé du Lemme de Kőnig nous sera-t-il utile au Chapitre 5, mais également les détails de la construction des branches minimales et maximales. On résume les propriétés importantes de la construction dans le Lemme suivant, tout en généralisant le résultat à des ensembles de branches quelconques (et pas seulement l'ensemble des branches infinies).

Lemme 1.9. *Soit $L \neq \varnothing$ un langage à branchements finis et $E \subseteq \partial L$ un ensemble non vide. Alors :*

1. *E a un supremum $\beta \in \partial L$, dénoté $\bigvee E$;*
2. *si β est une branche finie, alors $\beta \in E$;*
3. *sinon, il y a une chaîne dénombrable $u_0 \sqsubset u_1 \sqsubset u_2 \sqsubset \ldots \in \downarrow L$ et une collection de branches $\{\beta_n\}_{n\in\mathbb{N}} \subseteq E$ telles que $\beta = \bigsqcup_{n\in\mathbb{N}} u_n$ et pour tout n, $u_n \sqsubset \beta_n$.*

Démonstration. On procède comme dans la preuve du Lemme de Kőnig. Soit $u_0 = \varepsilon$ et, puisque $E \neq \varnothing$, prenons une branche $\beta_0 \in E$ quelconque. Notons qu'on a $u_0 \in \downarrow L$ puisque $L \neq \varnothing$, et on a aussi $u_0 \sqsubseteq \beta_0$.

Maintenant, supposons qu'on a défini $u_n \in \downarrow L$ et $\beta_n \in E$ tels que $u_n \sqsubseteq \beta_n$. Si $u_n = \beta_n$, alors on pose $\beta = \beta_n$ et on a terminé. Sinon, il existe $a \in A$ tel que $u_n \cdot a \sqsubseteq \beta_n$. Donc, l'ensemble

$$X_n = \{a \in A : \exists \alpha \in E \text{ t. q. } u_n \cdot a \sqsubseteq \alpha\}$$

n'est pas vide et, puisque L est à branchements finis, X_n est un ensemble fini. Soit donc $\overline{a} = \max(X_n)$ et $u_{n+1} = u_n \cdot \overline{a}$. Puisque $\overline{a} \in X_n$, on peut choisir $\beta_{n+1} \in E$ tel que $u_{n+1} \sqsubseteq \beta_{n+1}$. Puisque $\beta_{n+1} \in \overline{L}$, on a donc $u_{n+1} \in \downarrow \overline{L} = \overline{\downarrow L}$ et puisque u_{n+1} est un mot fini, $u_{n+1} \in \downarrow L$.

En procédant de cette manière tant que possible, soit la construction s'arrête à l'étape n avec $\beta = u_n \in E$, ou bien on construit une chaîne dénombrable $u_0 \sqsubset u_1 \sqsubset u_2 \sqsubset \ldots \in \downarrow L$ telle que pour tout n, il existe $\beta_n \in E$ avec $u_n \sqsubset \beta_n$. Dans ce cas, on pose $\beta = \bigsqcup_{n\in\mathbb{N}} u_n$. En particulier, le seul cas où β peut être fini implique $\beta \in E$. Il reste seulement à montrer que, tant dans le cas fini que dans le cas infini, on a $\beta = \bigvee E$.

Montrons d'abord que β est un majorant. Supposons le contraire : soit $\gamma \in E$ tel que $\beta \prec \gamma$. Soit $w = \beta \sqcap \gamma$ et $n = |w|$. Alors par construction, $w = u_n$. Or,

puisque $\beta \prec \gamma$, il existe $a, b \in A$ tels que $a < b$, $u_n \cdot a \sqsubseteq \beta$ et $u_n \cdot b \sqsubseteq \gamma$. Mais alors, $u_n \cdot a = u_{n+1}$ et par construction, $a = \max(X_n)$. Or, puisque $\gamma \in E$, on a $b \in X_n$ et puisque $a < b$, on rencontre une contradiction.

Il ne reste plus qu'à montrer que β est le plus petit des majorants. Soit donc $\gamma \prec \beta$ une branche quelconque. Comme plus haut, il existe $n \in \mathbb{N}$ et $a, b \in A$ tels que $a < b$, $u_n \cdot a \sqsubseteq \gamma$ et $u_n \cdot b \sqsubseteq \beta$. Or, par construction, $u_n \cdot b = u_{n+1} \sqsubseteq \beta_{n+1}$. Donc $\gamma \prec \beta_{n+1}$ et γ n'est pas un majorant de E. □

Remarquons que, bien que les deux preuves soient très similaires, le Lemme 1.9 n'implique pas directement le Lemme de Kőnig, puisqu'il faut d'abord démontrer que l'ensemble E des branches infinies de L est non vide, afin d'invoquer le Lemme 1.9. Or c'est là l'énoncé même du Lemme de Kőnig classique (Perrin et Pin, 2004, Chap. I, Prop. 2.2).

Lemme 1.10. *Dans l'énoncé du Lemme 1.9, si $\beta \notin E$, alors on peut supposer sans perte de généralité que pour tout n, $\beta_n \prec \beta_{n+1}$ et $u_n = \beta_n \sqcap \beta_{n+1}$.*

Démonstration. Soit β, $(\beta_n)_{n\in\mathbb{N}}$ et $(u_n)_{n\in\mathbb{N}}$ comme dans le Lemme 1.9. Quitte à rajouter des préfixes entre les u_n, on peut admettre sans perte de généralité que pour tout n, $|u_n| = n$ (c'est d'ailleurs le cas dans notre preuve du Lemme 1.9).

Si $\beta \notin E$, alors pour tout n, $\beta \neq \beta_n$ et donc $\beta \sqcap \beta_n$ est un mot fini. Soit $f(n) = |\beta \sqcap \beta_n|$. On a donc $u_{f(n)} = \beta \sqcap \beta_n$ pour tout n. Remarquons, de plus, que pour tout n, puisque $u_n \sqsubseteq \beta$ et $u_n \sqsubseteq \beta_n$, alors $u_n \sqsubseteq \beta \sqcap \beta_n$. On trouve donc $n = |u_n| \leq |\beta \sqcap \beta_n| = f(n)$. En particulier, la fonction f n'est pas bornée. On peut donc trouver $n_0 < n_1 < n_2 < \ldots \in \mathbb{N}$ tels que pour tout i, $f(n_i) < f(n_{i+1})$. Pour tout $i \in \mathbb{N}$, soit $\widetilde{\beta}_i := \beta_{n_i}$ et $\widetilde{u}_i := u_{f(n_i)}$. On veut montrer que les collections $(\widetilde{\beta}_i)_{i\in\mathbb{N}}$ et $(\widetilde{u}_i)_{i\in\mathbb{N}}$ ont les propriétés voulues.

D'abord, pour tout $i \in \mathbb{N}$, $\widetilde{u}_i = u_{f(n_i)} = \beta \sqcap \beta_{n_i} = \beta \sqcap \widetilde{\beta}_i \sqsubseteq \widetilde{\beta}_i$. Aussi, on a $\widetilde{u}_i = u_{f(n_i)} \sqsubset u_{f(n_{i+1})} = \widetilde{u}_{i+1}$ et donc, les $\widetilde{u}_i$ forment une chaîne croissante. De plus, puisque la chaîne des u_n est croissante, on a

$$\beta = \bigsqcup_{n\in\mathbb{N}} u_n = \bigsqcup_{i\in\mathbb{N}} \bigsqcup_{k\leq f(n_i)} u_k = \bigsqcup_{i\in\mathbb{N}} u_{f(n_i)} = \bigsqcup_{i\in\mathbb{N}} \widetilde{u}_i.$$

Ainsi, la partie 3 du Lemme 1.9 est satisfaite.

Fixons maintenant $i \in \mathbb{N}$. Puisque $\widetilde{u}_i = \beta \sqcap \widetilde{\beta}_i$ et $\widetilde{\beta}_i \prec \beta$, alors il existe $a, b \in A$ tels que $a < b$, $\widetilde{u}_i \cdot a \sqsubseteq \widetilde{\beta}_i$ et $\widetilde{u}_i \cdot b \sqsubseteq \beta$. Enfin, puisque $\widetilde{u}_i \sqsubset \widetilde{u}_{i+1} \sqsubset \beta$, alors $\widetilde{u}_i \cdot b \sqsubseteq \widetilde{u}_{i+1} \sqsubseteq \widetilde{\beta}_{i+1}$. Il s'ensuit que $\widetilde{u}_i = \widetilde{\beta}_i \sqcap \widetilde{\beta}_{i+1}$ et $\widetilde{\beta}_i \prec \widetilde{\beta}_{i+1}$, tel que souhaité. □

Bien sûr, un énoncé dual à celui des Lemmes 1.9 et 1.10 est également vrai. Une conséquence immédiate de cela est que l'ensemble ordonné $(\partial L, \preceq)$ est un treillis complet.

Proposition 1.11. *Soit $L \neq \varnothing$ un langage à branchements finis et $E \subseteq \partial L$. Alors E admet un infimum $\bigwedge E \in \partial L$ ainsi qu'un supremum $\bigvee E \in \partial L$.*

Démonstration. Traitons d'abord le cas $E \neq \varnothing$. L'existence de $\bigvee E$ est garantie par le Lemme 1.9. Soit L' le même langage que L, mais sur l'alphabet A^{op} (c'est-à-dire A avec la relation d'ordre intervertie). Alors l'ordre $\preceq$ est lui-même interverti et donc le supremum de E dans $\partial L'$ est l'infimum de E dans ∂L.

Il reste à considérer le cas $E = \varnothing$. Puisque chaque $\beta \in \partial L$ est un minorant de $\varnothing$, alors $\bigwedge \varnothing = \bigvee \partial L$. De la même façon, $\bigvee \varnothing = \bigwedge \partial L$. □

1.4 Graphes étiquetés

Un ***graphe étiqueté*** est un triplet $G = \langle V, A, \varsigma \rangle$ où V est un ensemble appelé ***support*** de G, A est un alphabet et $\varsigma \subseteq V \times A \times V$ est appelé ***relation de***

transition. Par abus de langage, le support V sera généralement dénoté par G comme le graphe, et ses éléments seront appelés des *sommets*. La notation $u \xrightarrow{a} v$ signifie $(u, a, v) \in \varsigma$. On dit alors que v est un ***successeur*** de u et que u est un ***prédécesseur*** de v.

Pour un sommet $u \in G$ l'ensemble des successeurs de u est dénoté $\mathrm{suc}(u)$ et son ***degré sortant***, dénoté $\deg(u)$, est le nombre de triplets de la forme (u, a, v) dans ς (où $a \in A$ et $v \in G$). On dit que G est un graphe à ***branchements finis*** si chaque sommet a un degré sortant fini.

On dit que G est ***déterministe*** si pour tout $u, v, v' \in G$ et $a \in A$, $u \xrightarrow{a} v$ et $u \xrightarrow{a} v'$ impliquent $v = v'$; dans ce cas, on écrira $v = \varsigma_a u$. Si, de plus, $\deg(u) = 1$, alors on se permettra d'omettre l'étiquette et d'écrire simplement $u \to v$ ou $v = \varsigma u$ sans ambiguité. Plus généralement, étant donné $u_0, u_1, \ldots, u_n \in G$ et $a_1, \ldots, a_n \in A$ tels que pour tout i, $u_{i-1} \xrightarrow{a_i} u_i$, on écrira $u_n = \varsigma_{a_1 \cdots a_n} u_0$.

Un ***chemin*** dans un graphe déterministe G est une paire $\Gamma = (u, \gamma)$ où $u \in V$ et $\gamma \in A^\infty$ sont tels que pour tout $n \leq |\gamma|$ (si γ est fini) ou bien pour tout $n \in \mathbb{N}$ (si γ est infini), $\Gamma(n) := \varsigma_{\gamma\restriction n} u$ est bien défini. La notation $v \in \Gamma$ signifie qu'il existe un certain n tel que $v = \Gamma(n)$. On dit que Γ est *fini* si $|\gamma| < \infty$, et qu'il est *infini* sinon. Le sommet u s'appelle la ***source*** de Γ et, si Γ est fini, $\varsigma_\gamma u$ est sa ***cible***. Si $0 < |\gamma| < \infty$ et $\Gamma(|\gamma|) = \Gamma(0)$, alors Γ est appelé ***cycle***. Deux chemins $\Gamma_0 = (u_0, \gamma_0)$ et $\Gamma_1 = (u_1, \gamma_1)$ sont dits *composables* si Γ_0 est fini et $\varsigma_{\gamma_0} u_0 = u_1$. Dans ce cas, on définit $\Gamma_0 \cdot \Gamma_1 = (u_0, \gamma_0 \cdot \gamma_1)$. On écrira $u \twoheadrightarrow v$ s'il existe un chemin fini dans G dont u est la source et v est la cible. S'il y a ambiguïté possible sur le graphe considéré, on pourra écrire $u \twoheadrightarrow_G v$ et $u \twoheadrightarrow_G v$ pour le préciser.

La relation $\twoheadrightarrow$ n'est pas, en général, une relation d'ordre sur G : elle n'est pas antisymétrique lorsque G contient un cycle non trivial. On peut toutefois l'utiliser pour ordonner les *composantes fortement connexes* de G.

Un sous-graphe $K \subseteq G$ est ***connexe*** si, pour tout $u, v \in K$, on a $u \twoheadrightarrow_K v$ ou $v \twoheadrightarrow_K u$. On dit que K est ***fortement connexe*** si on a, à la fois, $u \twoheadrightarrow_K v$ et $v \twoheadrightarrow_K u$, pour tout $u, v \in K$. Une ***composante (fortement) connexe*** est un sous-graphe (fortement) connexe non vide maximal, en ce sens qu'il n'existe aucun autre sous-graphe (fortement) connexe K' de G tel que $K \subset K'$. On dira d'un sous-graphe (fortement) connexe qu'il est ***trivial*** s'il ne contient qu'un seul sommet.

Soit $\mathcal{K}$ l'ensemble des composantes fortement connexes de G. On écrit $K \Rightarrow K'$ s'il existe $u \in K$ et $v \in K'$ tels que $u \twoheadrightarrow_G v$.

Proposition 1.12. *La relation $\Rightarrow$ est une relation d'ordre sur $\mathcal{K}$.*

Démonstration.

- *Réflexivité* : Soit $K \in \mathcal{K}$ et $v \in K$. Puisque $v \twoheadrightarrow v$, alors $K \Rightarrow K$.
- *Transitivité* : Soit $K_1 \Rightarrow K_2 \Rightarrow K_3$. Alors il existe $u \in K_1$ et $v \in K_2$ tels que $u \twoheadrightarrow v$ et il existe aussi $v' \in K_2$ et $w \in K_3$ tels que $v' \twoheadrightarrow w$. Mais puisque $v, v' \in K_2$, alors $v \twoheadrightarrow v'$. On a donc $u \twoheadrightarrow v \twoheadrightarrow v' \twoheadrightarrow w$. On en conclut, par transitivité de $\twoheadrightarrow$, qu'on a $u \twoheadrightarrow w$ et donc $K_1 \Rightarrow K_3$.
- *Antisymétrie* : Soit $K_1, K_2 \in \mathcal{K}$ tels que $K_1 \Rightarrow K_2$ et $K_2 \Rightarrow K_1$. Alors il existe $u \in K_1$ et $v \in K_2$ tels que $u \twoheadrightarrow v$ et il existe aussi $w \in K_2$ et $z \in K_1$ tels que $w \twoheadrightarrow z$. Mais puisque $v, w \in K_2$, alors $v \twoheadrightarrow w$ et, puisque $u, z \in K_1$, alors $z \twoheadrightarrow u$. On a donc $v \twoheadrightarrow w \twoheadrightarrow z \twoheadrightarrow u$, d'où que u et v doivent appartenir à la même composante fortement connexe, c'est-à-dire, $K_1 = K_2$. □

1.5 Arbres et langages

Un graphe étiqueté déterministe G est un ***arbre*** s'il existe un sommet $r \in G$ (la ***racine***, qu'on dénotera également $\sqrt{G}$) tel que pour tout $u \in G$, il existe

un unique $w \in A^*$ tel que $u = \varsigma_w r$. Remarquons que, dans ce cas, la fonction $\ell : G \to A^*$ qui envoie chaque $u \in G$ sur le w correspondant est injective. G est donc en bijection avec le langage $\ell(G)$, qui est préfixe-clos, par une conséquence immédiate de la définition d'un chemin dans G. Réciproquement, étant donné n'importe quel langage préfixe-clos $L \subseteq A^*$, soit $\alpha(L) = \langle L, A, \varsigma \rangle$ où $(u, a, v) \in \varsigma$ si et seulement si $v = u \cdot a$. Alors L et $\alpha(L)$ sont en bijection (parce que L est le support) et on vérifie facilement que l'inverse de α est ℓ.

Cette correspondance entre les arbres et les langages préfixe-clos nous permettra de *ne faire aucune différence* entre les deux concepts dans les chapitres suivants. Cela nous permettra donc d'utiliser la notation des langages pour traiter d'arbres et vice-versa, justifiant ainsi d'avoir fait le choix d'un vocabulaire arboricole (*branches* et *branchements*) à la section 1.3, ainsi que l'intuition géométrique qui s'en dégage.

Notons qu'à tout langage $L \subseteq A^*$ (pas nécessairement préfixe-clos) correspond un sous-graphe de l'*arbre* $\downarrow L$, dont les transitions sont, encore une fois, les suivantes :

$$u \xrightarrow{a} v \iff v = u \cdot a \,.$$

Il va de soi que, dans ce graphe, $u \twoheadrightarrow v$ implique $u \sqsubseteq v$. Les composantes fortement connexes du graphe sont donc toutes triviales, par antisymétrie de $\sqsubseteq$. On s'intéresse alors plutôt à l'ensemble $\widetilde{\mathcal{K}}$ des composantes connexes d'un langage L. Ces composantes sont, à leur tour, des arbres. Par abus de langage, pour $K, K' \in \widetilde{\mathcal{K}}$, on écrit $K \sqsubseteq K'$ s'il existe $u \in K$ et $v \in K'$ tels que $u \sqsubseteq v$.

Proposition 1.13. *La relation $\sqsubseteq$ est une relation d'ordre sur $\widetilde{\mathcal{K}}$.*

Démonstration.

– *Réflexivité.* Soit $K \in \widetilde{\mathcal{K}}$ et $v \in K$. Puisque $v \sqsubseteq v$, alors $K \sqsubseteq K$.

– *Antisymétrie.* Supposons $K_1 \sqsubseteq K_2$ et $K_2 \sqsubseteq K_1$. Soit $u \in K_1$ et $v \in K_2$ tels que $u \sqsubseteq v$ et soit $w \in K_2$ et $z \in K_1$ tels que $w \sqsubseteq z$. Puisque $u, z \in K_1$, alors $u \twoheadrightarrow_{K_1} z$ ou $z \twoheadrightarrow_{K_1} u$. De la même façon, puisque $v, w \in K_2$, alors $v \twoheadrightarrow_{K_2} w$ ou $w \twoheadrightarrow_{K_2} v$.

Si $v \twoheadrightarrow_{K_2} w$, alors on déduit $u \sqsubseteq v \sqsubseteq w \sqsubseteq z$ et donc, $u \twoheadrightarrow_{K_1} z$ (parce que Ψ est un arbre et il n'y a donc qu'un seul chemin possible entre u et z). Puisque v et w font partie de ce chemin, alors $v, w \in K_1$ et, en particulier, $K_1 = K_2$. De la même façon, si $z \twoheadrightarrow_{K_1} u$, on peut déduire $u, z \in K_1$ et donc $K_1 = K_2$.

Supposons enfin $w \twoheadrightarrow_{K_2} v$ et $u \twoheadrightarrow_{K_1} z$. On a donc $u \sqsubseteq z$ et, par définition, $w \sqsubseteq z$ d'ou on conclut, par le Lemme 1.2, qu'on a soit $u \sqsubseteq w$, ou alors $w \sqsubseteq u$. Si $u \sqsubseteq w \sqsubseteq z$, alors puisque $u \twoheadrightarrow_{K_1} z$, on conclut $w \in K_1$ et donc $K_1 = K_2$. De la même manière, si $w \sqsubseteq u \sqsubseteq v$, alors de $w \twoheadrightarrow_{K_2} v$, on conclut $u \in K_2$ et donc $K_1 = K_2$.

– *Transitivité.* Supposons $K_1 \sqsubseteq K_2 \sqsubseteq K_3$. Soit $u \in K_1$ et $v \in K_2$ tels que $u \sqsubseteq v$ et soit $v' \in K_2$ et $w \in K_3$ tels que $v' \sqsubseteq w$.

Puisque $v, v' \in K_2$, alors il y a deux possibilités. La première est $v \twoheadrightarrow_{K_2} v'$, auquel cas on déduit directement $u \sqsubseteq v \sqsubseteq v' \sqsubseteq w$ et donc $K_1 \sqsubseteq K_3$.

Sinon, on a $v' \twoheadrightarrow_{K_2} v$. Par le Lemme 1.2, on a donc soit $u \sqsubseteq v'$ ou bien $v' \sqsubseteq u$. Dans le premier cas, on a donc $u \sqsubseteq v' \sqsubseteq w$ et alors $K_1 \sqsubseteq K_3$. Dans le second, on obtient $K_2 \sqsubseteq K_1$ et donc, par antisymétrie, $K_1 = K_2$. Mais puisque $K_2 \sqsubseteq K_3$, on conclut $K_1 \sqsubseteq K_3$. □

CHAPITRE II

CATÉGORIES ET POINTS FIXES

Ce chapitre est une introduction aux notions de théorie des catégories qui seront utiles dans les autres chapitres de cette thèse. La section 2.1 établit simplement les notations, relatives aux catégories, qui seront utilisées par la suite et fait le point sur les connaissances qui sont attendues de la part du lecteur. Quant aux sections 2.2 à 2.4, elles établissent la version catégorique de la théorie des points fixes, qui modélise notamment l'induction et la coinduction en programmation fonctionnelle. Un bon tutoriel des notions d'induction et de coinduction traitées dans ces sections est (Jacobs et Rutten, 1997), toutefois complété ici pour cadrer avec les systèmes dirigés d'équations, introduits dans (Santocanale, 2001) et revus (avec une nouvelle présentation) dans (Fortier et Santocanale, 2013). Ensuite, à la section 2.5, on décrit une solution canonique aux systèmes dirigés d'équations dans la catégorie des ensembles, telle que démontrée dans (Santocanale, 2002b). Enfin, la section 2.6 décrit le cadre général dans lequel on peut interpréter les systèmes dirigés d'équations, soit celui des catégories μ-bicomplètes.

2.1 Ce qu'il faut savoir sur les catégories

Pour le néophyte, il faut savoir qu'une catégorie $\mathcal{C}$ est un graphe orienté (possiblement *très* infini) dont chaque sommet $A \in \mathcal{C}$ (ci-dessous appelé ***objet***) est

muni d'une ***flèche identité*** $\mathtt{id}_A : A \to A$. Étant donné deux flèches $f : A \to B$ et $g : B \to C$, on doit avoir défini leur ***composition*** $f \cdot g : A \to C$ de sorte que les propriétés suivantes soient satisfaites.

Associativité. $f \cdot (g \cdot h) = (f \cdot g) \cdot h$, pour toutes flèches f, g, h composables.

Éléments neutres. $\mathtt{id}_A \cdot f = f = f \cdot \mathtt{id}_B$, pour tout $f : A \to B$.

Un exemple primordial de catégorie est donné par la catégorie $\mathcal{Ens}$, dont les objets sont les ensembles et les flèches sont les fonctions (la source et la cible de ces flèches sont respectivement le domaine et le codomaine).

Notons que, pour des raisons visuelles et contrairement à ce qui est souvent présenté, on prendra l'habitude de composer les fonctions (et les flèches en général) dans la direction vers laquelle elles pointent et en utilisant l'opérateur $'\cdot'$. L'usage est plutôt (à cause de l'importance de la catégorie $\mathcal{Ens}$) de dénoter la composition par $'\circ'$ et de composer à rebours. On suivra toutefois cette dernière convention pour la composition de foncteurs ou pour le passage d'un argument (qui se fera à droite). En résumé :

$$(f \cdot g)(x) = (g \circ f)(x) = g(f(x)).$$

Du reste, puisque cette thèse n'est pas un ouvrage d'introduction aux catégories, on prendra pour acquis que le lecteur soucieux d'en comprendre les détails possède au moins une connaissance de base en théorie des catégories. Une telle connaissance peut être acquise dans l'excellent livre de Awodey (2006) ou encore dans les premiers chapitres de (Mac Lane, 1998).

Plus précisément, on n'introduira pas les concepts suivants, qui seront réputés familiers : diagramme commutatif, foncteur, transformation naturelle, objet initial, objet final, produit (cartésien), coproduit, catégorie bicartésienne et catégorie opposée (qu'on dénotera $\overline{\mathcal{C}}$ plutôt que $\mathcal{C}^{op}$). Le lecteur est, d'ailleurs, présumé à l'aise avec le principe de dualité.

Au plan des notations, un objet initial sera généralement dénoté $\mathbf{0}$ et l'unique flèche $\mathbf{0} \to A$ sera dénotée $?_A$. Un objet final, quant à lui, sera dénoté par $\mathbf{1}$ et l'unique flèche qu'il impose pour chaque objet sera dénotée $!_A : A \to \mathbf{1}$. Quant aux notations relatives aux produits et coproduits, on peut les retrouver dans les diagrammes commutatifs suivants.

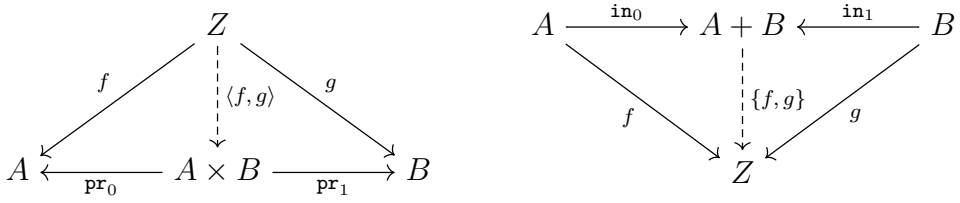


Figure 2.1 Diagrammes du produit et du coproduit

De plus, étant donné deux ensembles $I \subseteq J$ et une collection d'objets $(A_j)_{j\in J}$ d'une catégorie $\mathcal{C}$, on dénote par $\mathtt{pr}_I^J : \prod_{j\in J} A_j \to \prod_{i\in I} A_i$ la projection canonique. Si $I = \{i\}$ est un singleton, on se permettra d'écrire $\mathtt{pr}_i^J$ au lieu de $\mathtt{pr}_{\{i\}}^J$. De façon duale, on définit $\mathtt{in}_I^J : \coprod_{i\in I} A_i \to \coprod_{j\in J} A_j$ comme étant l'injection canonique.

Si $\mathcal{C}$ est une catégorie localement petite, alors étant donné deux objets $A, B \in \mathcal{C}$, l'ensemble des flèches $f : A \to B$ est dénoté $\mathcal{C}(A, B)$, au lieu de $\hom_{\mathcal{C}}(A, B)$ comme c'est souvent le cas. Rappelons que $\mathcal{C}(\_, \_) : \overline{\mathcal{C}} \times \mathcal{C} \to \mathcal{Ens}$ est un foncteur. On peut généraliser cette notation comme suit. Étant donné deux foncteurs $F : \mathcal{D}_0 \to \mathcal{C}$ et $G : \mathcal{D}_1 \to \mathcal{C}$, soit $\mathcal{C}(F, G)$ le foncteur défini par la composition suivante :

$$\overline{\mathcal{D}_0} \times \mathcal{D}_1 \xrightarrow{\overline{F}\times G} \overline{\mathcal{C}} \times \mathcal{C} \xrightarrow{\mathcal{C}(\_,\_)} \mathcal{Ens}\,.$$

Pour plus de clarté, décrivons l'action de $\mathcal{C}(F, G)$ sur les objets et les flèches de $\overline{\mathcal{D}_0} \times \mathcal{D}_1$. On dénotera ces objets $x = (\overline{x_0}, x_1)$ ou $y = (\overline{y_0}, y_1)$ pour $x_0, y_0 \in \mathcal{D}_0$ et $x_1, y_1 \in \mathcal{D}_1$. On a alors $\mathcal{C}(F, G)(x) = \mathcal{C}(Fx_0, Gx_1)$ et similairement pour y.

Une flèche $f : x \to y$ de $\overline{\mathcal{D}_0} \times \mathcal{D}_1$ est de la forme $f = (\overline{u}, v)$ où $u : y_0 \to x_0$ est une flèche de $\mathcal{D}_0$ et $v : x_1 \to y_1$ est une flèche de $\mathcal{D}_1$. On décrit alors $\mathcal{C}(F,G)(f) : \mathcal{C}(Fx_0, Gx_1) \to \mathcal{C}(Fy_0, Gy_1)$ comme la fonction qui envoie chaque $h \in \mathcal{C}(Fx_0, Gx_1)$ sur la composition suivante :

$$Fy_0 \xrightarrow{Fu} Fx_0 \xrightarrow{h} Gx_1 \xrightarrow{Gv} Gy_1.$$

Lemme 2.1. *Soit I un ensemble d'indices et $\mathcal{C}$ une catégorie localement petite. Pour tout $i \in I$, soit $F_i : \mathcal{D}_0 \to \mathcal{C}$ et $G_i : \mathcal{D}_1 \to \mathcal{C}$ des foncteurs. Soit enfin*

$$F = (F_i)_{i\in I} : \mathcal{D}_0 \to \mathcal{C}^I \qquad , \qquad G = (G_i)_{i\in I} : \mathcal{D}_1 \to \mathcal{C}^I \,.$$

Alors

$$\prod_{i\in I} \mathcal{C}(F_i, G_i) = \mathcal{C}^I(F,G)\,.$$

Démonstration. Il suffit de dérouler la définition de chacun des deux foncteurs (à gauche et à droite de l'égalité) et de comparer les résultats sur les objets et les flèches de $\overline{\mathcal{D}_0} \times \mathcal{D}_1$. Commençons par le foncteur du côté gauche.

– *Objets.* Soit $x = (\overline{x_0}, x_1) \in \overline{\mathcal{D}_0} \times \mathcal{D}_1$. Alors on a

$$\begin{aligned}\Big(\prod_{i\in I} \mathcal{C}(F_i, G_i)\Big)(x) &= \prod_{i\in I} \Big(\mathcal{C}(F_i, G_i)(x)\Big) \\ &= \prod_{i\in I} \mathcal{C}(F_i x_0, G_i x_1) \\ &= \big\{\vec{h} = (h_i)_{i\in I} : \forall i, h_i \in \mathcal{C}(F_i x_0, G_i x_1)\big\}.\end{aligned}$$

– *Flèches.* Soit $f = (\overline{u}, v) : x \to y$ une flèche de $\overline{\mathcal{D}_0} \times \mathcal{D}_1$. Alors pour tout $\vec{h} = (h_i)_{i\in I} \in \prod_{i\in I} \mathcal{C}(F_i, G_i)(x)$, on a

$$\begin{aligned}\Big(\prod_{i\in I} \mathcal{C}(F_i, G_i)(f)\Big)(h) &= \Big(\big(\mathcal{C}(F_i, G_i)(f)\big)(h_i)\Big)_{i\in I} \\ &= \big(F_i u \cdot h_i \cdot G_i v\big)_{i\in I}\,.\end{aligned}$$

Procédons maintenant au même exercice pour le côté droit de l'équation.

– *Objets.* Soit $x = (\overline{x_0}, x_1) \in \overline{\mathcal{D}_0} \times \mathcal{D}_1$. Alors on a

$$\begin{aligned}\big(\mathcal{C}^I(F,G)\big)(x) &= \mathcal{C}^I(Fx_0, Gx_1)\\ &= \mathcal{C}^I\big((F_ix_0)_{i\in I}, (G_ix_1)_{i\in I}\big)\\ &= \big\{\vec{h} = (h_i)_{i\in I} : \forall i, h_i \in \mathcal{C}(F_ix_0, G_ix_1)\big\}.\end{aligned}$$

– *Flèches.* Soit $f = (\overline{u}, v) : x \to y$ une flèche de $\overline{\mathcal{D}_0} \times \mathcal{D}_1$. Alors pour tout $\vec{h} = (h_i)_{i\in I} \in \mathcal{C}^I(F,G)(x)$, on a

$$\begin{aligned}\big(\mathcal{C}^I(F,G)(f)\big)(h) &= Fu \cdot h \cdot Gv\\ &= (F_iu)_{i\in I} \cdot (h_i)_{i\in I} \cdot (G_iv)_{i\in I}\\ &= \big(F_iu \cdot h_i \cdot G_iv\big)_{i\in I}.\end{aligned}$$

□

2.2 Algèbres initiales et induction

Définition. Soit $F : \mathcal{C} \to \mathcal{C}$ un endofoncteur. Une ***F*-algèbre** est une paire (A, a) où A est un objet de $\mathcal{C}$ et $a : F(A) \to A$ est une flèche de $\mathcal{C}$. On dit alors que A est le ***support*** et a est la ***structure*** de l'algèbre.

Exemple 1. La plupart des structures algébriques définies couramment en mathématiques sont des algèbres dans le sens présent. Par exemple, un groupe est un ensemble A (le support) muni d'un élément choisi (l'élément neutre), c'est-à-dire une flèche $e : \mathbf{1} \to A$ dans $\mathcal{Ens}$, d'une opération d'inversion $(-)^{-1} : A \to A$ puis d'une opération binaire $* : A \times A \to A$ satisfaisant certains axiomes. La structure algébrique naît donc de ces trois fonctions, e, $(-)^{-1}$ et $*$, ou de façon équivalente, de la fonction suivante.

$$a = \{e, (-)^{-1}, *\} : \mathbf{1} + A + (A \times A) \to A$$

La paire (A, a) est alors une algèbre du foncteur $F(X) = \mathbf{1} + X + (X \times X)$. ■

Étant donné un endofoncteur $F : \mathcal{C} \to \mathcal{C}$, on peut former la catégorie $\mathcal{Alg}(F)$ dont les objets sont les F-algèbres, et dont les flèches $f : (A, a) \to (B, b)$ sont les flèches f de $\mathcal{C}$ pour lesquelles le diagramme suivant commute :

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ {\scriptstyle a}\downarrow & & \downarrow{\scriptstyle b} \\ A & \xrightarrow[f]{} & B \end{array} \quad .$$

La structure de catégorie de $\mathcal{Alg}(F)$ est alors induite par celle de $\mathcal{C}$. Une ***F-algèbre initiale*** est simplement un objet initial de la catégorie $\mathcal{Alg}(F)$.

Exemple 2. Considérons par exemple (toujours dans $\mathcal{Ens}$), l'algèbre des nombres naturels, donnée par le choix d'un élément $0 : \mathbf{1} \to \mathbb{N}$ et d'une opération *successeur*, $\mathtt{Suc} : \mathbb{N} \to \mathbb{N}$. Il s'agit donc d'une algèbre du foncteur $F(X) = \mathbf{1} + X$. Il s'agit en fait de la F-algèbre initiale, puisqu'étant donné une autre F-algèbre $\mathbf{1} + A \xrightarrow{\{z,g\}} A$, on peut définir une *unique* fonction f faisant commuter le diagramme ci-dessous (c'est définir f par *induction sur* $\mathbb{N}$) :

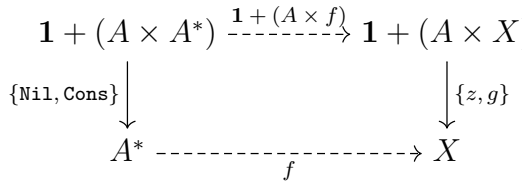
$$\begin{array}{ccc} \mathbf{1} + \mathbb{N} & \overset{\mathbf{1}+f}{\dashrightarrow} & \mathbf{1} + A \\ {\scriptstyle \{0,\mathtt{Suc}\}}\downarrow & & \downarrow{\scriptstyle \{z,g\}} \\ \mathbb{N} & \underset{f}{\dashrightarrow} & A \end{array} \qquad \begin{aligned} f(0) &= z\,, \\ f(\mathtt{Suc}\ n) &= g(f(n))\,. \end{aligned}$$

■

Plus généralement, la propriété universelle des algèbres initiales encode le concept d'*induction structurelle*.

Exemple 3. Toujours dans la catégorie des ensembles, soit $F(X) = \mathbf{1} + (A \times X)$, où A est un ensemble fixé. La F-algèbre initiale est le monoïde libre A^* (vu à la Section 1.1) dont la structure est donnée par une fonction $\mathtt{Nil} : \mathbf{1} \to A^*$ dont l'image est le mot vide ε et la fonction $\mathtt{Cons} : A \times A^* \to A^*$ (appelée *constructeur*) définie par $\mathtt{Cons}(a, u) = a{:}u$. La propriété universelle de cette algèbre initiale

permet de définir des fonctions par induction sur les mots, via le diagramme commutatif suivant :



$$f(\varepsilon) = z\,,$$
$$f(a{:}w) = g(a, f(w))\,.$$

■

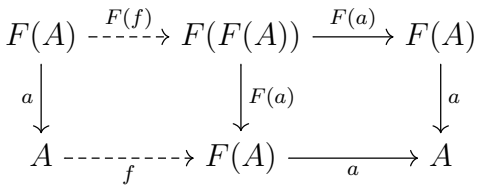
Exemple 4. Changeons un peu de catégorie. Rappelons qu'un *treillis complet* est un ensemble partiellement ordonné $(T, \leq)$ tel que chaque sous-ensemble $E \subseteq T$ admet un infimum et un supremum. Or, les ensembles partiellement ordonnés correspondent à des catégories $\mathcal{T}$ dont les objets sont les éléments de T, et dont il existe une et une seule flèche $f_{a,b} : a \to b$ si et seulement si $a \leq b$ (Awodey, 2006, §1.4). Un endofoncteur $F : \mathcal{T} \to \mathcal{T}$ est alors, tout simplement, une fonction croissante de T vers T.

Étant donné un tel foncteur, en déroulant la définition d'une F-algèbre, on constate qu'il s'agit simplement un élément $x \in T$ tel que $F(x) \leq x$, c'est-à-dire s'il s'agit d'un *point préfixe*. Le point x est la F-algèbre initiale si, pour tout autre point préfixe y, on a $x \leq y$. En d'autres mots, l'algèbre initiale est le point $x = \inf\{y \in T : F(y) \leq y\}$, qui existe parce que T est complet. ■

Lemme 2.2 (Lambek, 1968)**.** *Soit $F : \mathcal{C} \to \mathcal{C}$ un endofoncteur qui admet une algèbre initiale (A, a). Alors la flèche $a : F(A) \to A$ est inversible.*

Démonstration. Considérons le diagramme suivant, où f est obtenue par la pro-

priété universelle des algèbres initiales :



Le carré gauche du diagramme commute par construction et le carré droit commute trivialement. Donc le rectangle extérieur commute. Par unicité, on trouve donc $f \cdot a = \mathtt{id}_A$. Ensuite, puisque le carré gauche est commutatif, on trouve

$$a \cdot f = F(f) \cdot F(a) = F(f \cdot a) = F(\mathtt{id}_A) = \mathtt{id}_{F(A)}\,. \qquad \square$$

En d'autres mots, le lemme de Lambek affirme que les F-algèbres initiales sont des *points fixes* de F (à isomorphisme près). Ainsi, on écrira « $A =_\mu F(A)$ » [†] pour indiquer que A est le support de l'algèbre initiale du foncteur F.

Définition. Soit $\mathcal{C}, \mathcal{D}$ deux catégories et $F : \mathcal{C} \times \mathcal{D} \to \mathcal{C}$ un foncteur. Supposons que pour chaque objet $D \in \mathcal{D}$, le foncteur $F(-, D) : \mathcal{C} \to \mathcal{C}$ admette une algèbre initiale (A_D, a_D). L'***algèbre initiale paramétrée*** de F est la paire (F^μ, α) où $F^\mu : \mathcal{D} \to \mathcal{C}$ est le foncteur défini comme suit :

– **Sur les objets :** Pour tout $D \in \mathcal{D}$, on pose $F^\mu(D) := A_D$;

– **Sur les flèches :** Pour tout $f : X \to Y$ dans $\mathcal{D}$, $F^\mu(f) : A_X \to A_Y$ est l'unique

---

†. La terminologie usuelle est plutôt celle du μ-calcul : « $A = \mu X.F(X)$ ». On préférera toutefois la nôtre car on souhaite représenter des structures plus complexes par des systèmes d'équations (voir Section 2.4).

flèche h qui fait commuter le diagramme suivant :

$$\begin{array}{ccc} F(A_X, X) & \xrightarrow{F(h,X)} & F(A_Y, X) \\ \Big\downarrow{\scriptstyle a_X} & & \Big\downarrow{\scriptstyle F(A_Y,f)} \\ & & F(A_Y, Y) \\ & & \Big\downarrow{\scriptstyle a_Y} \\ A_X & \xrightarrow[h]{} & A_Y \end{array} \quad ;$$

et où $\alpha : F(F^\mu -, -) \to F^\mu$ est la transformation naturelle $\alpha = (a_D)_{D \in \mathcal{D}}$.

Exemple 5. Soit $F : \mathcal{Ens} \times \mathcal{Ens} \to \mathcal{Ens}$ le foncteur $F(X, Y) = \mathbf{1} + (Y \times X)$. Par l'Exemple 3, pour tout ensemble Y, l'algèbre initiale du foncteur $F(-, Y)$ est le monoïde libre Y^* avec la structure suivante :

$$\{\texttt{Nil}, \texttt{Cons}\} : \mathbf{1} + (Y \times Y^*) \to Y^* \,.$$

L'algèbre initiale paramétrée de F est donc le foncteur $F^\mu(Y) = Y^*$ et, pour tout $f : A \to B$, $F^\mu(f) : A^* \to B^*$ est la fonction définie comme suit :

$$\begin{array}{ccc} \mathbf{1} + (A \times A^*) & \xrightarrow{\mathbf{1} + A \times F^\mu(f)} & 1 + (A \times B^*) \\ & & \Big\downarrow{\scriptstyle 1 + (f \times B^*)} \\ \Big\downarrow{\scriptstyle \{\texttt{Nil},\texttt{Cons}\}} & & 1 + (B \times B^*) \\ & & \Big\downarrow{\scriptstyle \{\texttt{Nil},\texttt{Cons}\}} \\ A^* & \xrightarrow[F^\mu(f)]{} & B^* \end{array} \qquad \begin{aligned} F^\mu(f)(\varepsilon) &= \varepsilon \\ F^\mu(f)(a{:}w) &= f(a){:}F^\mu(f)(w)\,. \end{aligned}$$

En d'autres mots, on a $F^\mu(f)$ est la fonction $\texttt{map}_f$ qui associe, à une liste d'éléments de A, la liste des images de ces éléments par f. ■

On aura besoin de deux propriétés des algèbres initiales paramétrées dans le cadre de cette thèse, apparaissant dans (Santocanale, 2001). La première, le Lemme de

Bekić, est un outil permettant de résoudre des systèmes d'équations fonctorielles du type

$$\left\{ \begin{array}{l} X =_\mu F(X,Y) \\ Y =_\mu G(X,Y) \end{array} \right\}$$

où $F : \mathcal{C} \times \mathcal{D} \to \mathcal{C}$ et $G : \mathcal{C} \times \mathcal{D} \to \mathcal{D}$ sont deux foncteurs. Le résultat dit que pour résoudre un tel système, il suffit de le résoudre d'abord en X, pour obtenir :

$$\left\{ \begin{array}{l} X = \ F^\mu(Y) \\ Y =_\mu G(X,Y) \end{array} \right\}$$

qu'on peut transformer, en substituant la première équation dans la seconde, en :

$$Y =_\mu G(F^\mu(Y), Y)\,.$$

Il ne reste plus ensuite qu'à résoudre cette équation en Y.

Lemme 2.3 (Bekić)**.** *Soit deux foncteurs, $F : \mathcal{C} \times \mathcal{D} \to \mathcal{C}$ et $G : \mathcal{C} \times \mathcal{D} \to \mathcal{D}$. Soit (F^μ, α) l'algèbre initiale paramétrée de F (dont on suppose l'existence) et supposons, de plus, qu'il existe $X \in \mathcal{C}$, $Y \in \mathcal{D}$ et deux flèches,*

$$x : F^\mu(Y) \to X \qquad et \qquad y : G(X,Y) \to Y\,,$$

tels que la paire $\big((X,Y),(x,y)\big)$ soit l'algèbre initiale du foncteur

$$\langle F^\mu \circ \mathtt{pr}_{\mathcal{D}}\,,\, G\rangle \;:\; \mathcal{C} \times \mathcal{D} \to \mathcal{C} \times \mathcal{D}\,.$$

Alors la paire $\big((F^\mu(Y),Y)\,,\,(f,g)\big)$, où

$$f = \alpha_Y \qquad et \qquad g = G(x,Y) \cdot y\,,$$

est l'algèbre initiale du foncteur $\langle F, G\rangle : \mathcal{C} \times \mathcal{D} \to \mathcal{C} \times \mathcal{D}$.

Démonstration. Voir (Santocanale, 2002b, Proposition 2.1). □

Au Chapitre 4, on travaillera avec des transformations naturelles $\beta_{X,Y}$ de la forme de l'équation (2.1) ci-dessous. Le résultat qui suit est un théorème d'existence d'un point fixe paramétré pour ces transformations.

Proposition 2.4. *Soit $\mathcal{C}, \mathcal{Y}, \mathcal{Z}$ trois catégories, dont $\mathcal{C}$ admet les produits finis. Soit F, G et Q trois foncteurs comme suit :*

$$\begin{aligned} F &: \mathcal{C} \times \mathcal{Y} \to \mathcal{C}\,, \\ G &: \mathcal{Z} \to \mathcal{C}\,, \\ Q &: \overline{\mathcal{C}} \times \overline{\mathcal{Y}} \times \mathcal{Z} \to \mathcal{E}ns\,. \end{aligned}$$

Considérons une transformation naturelle en $x \in \mathcal{C}$, $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ de la forme suivante :

$$\vartheta_{x,y,z} : \mathcal{C}(x, Gz) \times Q(x, y, z) \to \mathcal{C}(F(x, y), Gz)\,. \tag{2.1}$$

Soit (F^μ, α) l'algèbre initiale paramétrée de F (dont on suppose l'existence).

Alors pour tout objet $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ et tout élément $q \in Q(F^\mu(y), y, z)$, il existe une unique flèche $f = f_{y,z}(q) \in \mathcal{C}(F^\mu(y), Gz)$ satisfaisant l'équation suivante :

$$\alpha_y \cdot f = \vartheta_{F^\mu(y),y,z}(f, q)\,,$$

où $\alpha_y : F(F^\mu(y), y) \to F^\mu(y)$ est la structure de l'algèbre initiale. De plus, la collection $(f_{y,z})_{y \in \mathcal{Y}, z \in \mathcal{Z}}$ est une transformation naturelle.

Démonstration. Il s'agit simplement, à un changement de variables près, de l'énoncé du Théorème 3.1 de (Santocanale, 2001). □

On aura, en fait, besoin d'une version vectorielle de cette dernière proposition.

Corollaire 2.5. *Soit $\mathcal{C}, \mathcal{Y}, \mathcal{Z}$ trois catégories, dont $\mathcal{C}$ admet les produits finis.*

Soit I un ensemble d'indices et F, Q deux foncteurs comme suit :

$$F : \mathcal{C}^I \times \mathcal{Y} \to \mathcal{C}^I \,,$$
$$Q : \overline{\mathcal{C}^I} \times \overline{\mathcal{Y}} \times \mathcal{Z} \to \mathcal{E}ns \,.$$

Soit aussi, pour tout $i \in I$, un foncteur $G_i : \mathcal{Z} \to \mathcal{C}$. Soit enfin ϑ une transformation naturelle en $x \in \mathcal{C}^I$, $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ de la forme suivante :

$$\vartheta_{x,y,z} : \prod_{i \in I} \mathcal{C}(\mathtt{pr}_i(x), G_i z) \times Q(x, y, z) \to \prod_{i \in I} \mathcal{C}(\mathtt{pr}_i \circ F(x, y), G_i z) \,.$$

Soit (F^μ, α) l'algèbre initiale paramétrée de F (dont on suppose l'existence).

Alors pour tout objet $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ et tout élément $q \in Q(F^\mu(y), y, z)$, il existe une unique flèche $f = f_{y,z}(q)$ de $\mathcal{C}^I$ satisfaisant l'équation suivante :

$$\alpha_y \cdot f = \vartheta_{F^\mu(y),y,z}(f, q) \,.$$

De plus, la collection $(f_{y,z})_{y \in \mathcal{Y}, z \in \mathcal{Z}}$ est une transformation naturelle.

Démonstration. Soit $G = \langle G_i \rangle_{i \in I} : \mathcal{Z} \to \mathcal{C}^I$. Pour tout $x \in \mathcal{C}^I$, on a trivialement $x = \big(\mathtt{pr}_i(x)\big)_{i \in I}$. Ainsi, par le Lemme 2.1, on a

$$\prod_{i \in I} \mathcal{C}(\mathtt{pr}_i(x), G_i z) = \mathcal{C}^I(x, Gz) \,,$$
$$\prod_{i \in I} \mathcal{C}(\mathtt{pr}_i \circ F(x, y), G_i z) = \mathcal{C}^I(F(x, y), Gz) \,.$$

Le résultat découle donc directement de la Proposition 2.4, avec $\mathcal{C}^I$ au lieu de $\mathcal{C}$.

□

2.3 Coalgèbres finales et coinduction

Une coalgèbre (finale) est simplement le dual d'une algèbre (initiale).

Définition. Soit $F : \mathcal{C} \to \mathcal{C}$ un endofoncteur. Une ***F*-coalgèbre** est une paire (Z, z) où Z est un objet de $\mathcal{C}$ et $z : Z \to F(Z)$ est une flèche de $\mathcal{C}$. On définit la catégorie $\mathcal{C}oalg(F)$ dont les objets sont les F-coalgèbres, et dont les flèches $f : (Z, z) \to (Y, y)$ sont les flèches f de $\mathcal{C}$ pour lesquelles le diagramme suivant commute :

$$\begin{array}{ccc} Z & \xrightarrow{\ f\ } & Y \\ {\scriptstyle z}\downarrow & & \downarrow{\scriptstyle y} \\ F(Z) & \xrightarrow[F(f)]{} & F(Y) \end{array} .$$

Une ***F*-coalgèbre finale** est un objet final de la catégorie $\mathcal{C}oalg(F)$.

Exemple 1. Dans la catégorie des ensembles, soit $F(X) = A \times X$, où A est un ensemble fixé. La F-coalgèbre finale est donnée par l'ensemble A^ω des mots infinis sur A, avec la structure $A^\omega \xrightarrow{\langle \mathtt{Head}, \mathtt{Tail} \rangle} A \times A^\omega$ (revoir la section 1.1). Étant donné une autre F-coalgèbre $Z \xrightarrow{\langle f, g \rangle} A \times Z$, la propriété universelle de la coalgèbre finale permet de définir la fonction $\mathrm{orb} : Z \to A^\omega$ qui associe, à chaque $z \in Z$, son *orbite observable* :

$$\begin{aligned} \mathtt{Head}(\mathrm{orb}(z)) &= f(z)\,, \\ \mathtt{Tail}(\mathrm{orb}(z)) &= \mathrm{orb}(g(z)). \end{aligned}$$

■

Exemple 2. Considérons, comme dans l'Exemple 4 de la Section 2.2, une catégorie $\mathcal{T}$ issue d'un treillis complet T. Une F-coalgèbre est, cette-fois, un point *postfixe*, c'est-à-dire un point $z \in T$ tel que $z \leq F(z)$. La F-coalgèbre finale est alors le point $z = \sup\{y \in T : y \leq F(y)\}$. ■

On peut, bien sûr, dualiser tout ce qu'on a dit sur les algèbres initiales à la Section 2.2 pour obtenir des résultats sur les coalgèbres finales. La coalgèbre finale paramétrée d'un foncteur $F : \mathcal{C} \times \mathcal{D} \to \mathcal{C}$ est dénotée $F^\nu : \mathcal{D} \to \mathcal{C}$. Prenons au moins l'espace nécessaire pour dualiser le Corollaire 2.5.

Lemme 2.6. *Soit $\mathcal{C}, \mathcal{Y}, \mathcal{Z}$ trois catégories, dont $\mathcal{C}$ admet les coproduits finis. Soit I un ensemble d'indices et G, Q deux foncteurs comme suit :*

$$G : \mathcal{C}^I \times \mathcal{Z} \to \mathcal{C}^I \,,$$
$$Q : \mathcal{C}^I \times \overline{\mathcal{Y}} \times \mathcal{Z} \to \mathcal{E}ns \,.$$

Soit aussi, pour tout $i \in I$, soit un foncteur $F_i : \mathcal{Y} \to \mathcal{C}$. Soit enfin ϑ une transformation naturelle en $x \in \mathcal{C}^I$, $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ de la forme suivante :

$$\vartheta_{x,y,z} : \prod_{i \in I} \mathcal{C}(F_i y \,,\, \mathtt{pr}_i(x)) \times Q(x,y,z) \to \prod_{i \in I} \mathcal{C}(F_i y \,,\, \mathtt{pr}_i \circ G(x,z)) \,.$$

Soit (G^ν, ζ) la coalgèbre finale paramétrée de G (dont on suppose l'existence).

Alors pour tout objet $y \in \mathcal{Y}$ et $z \in \mathcal{Z}$ et tout élément $q \in Q(G^\nu(z), y, z)$, il existe une unique flèche $g = g_{y,z}(q)$ de $\mathcal{C}^I$ satisfaisant l'équation suivante :

$$g \cdot \zeta_z = \vartheta_{G^\nu(z),y,z}(g, q) \,.$$

où $\zeta_z : G^\nu(z) \to G(G^\nu(z), z)$ est la structure de l'algèbre initiale. De plus, la collection $(g_{y,z})_{y \in \mathcal{Y}, z \in \mathcal{Z}}$ est une transformation naturelle.

L'objectif ici est plutôt de parler du *principe de coinduction*, qui est le principe de preuve associé aux coalgèbres finales dans la catégorie des ensembles (en opposition au *principe d'induction* des algèbres initiales).

Définition. Soit (Z, z) une F-coalgèbre dans la catégorie $\mathcal{E}ns$. Une ***bisimulation*** sur Z est une relation $R \subseteq Z \times Z$ munie d'une structure de F-coalgèbre $\gamma : R \to F(R)$ telle que le diagramme suivant commute :

$$\begin{array}{ccccc} Z & \xleftarrow{\mathtt{pr}_0 \restriction_R} & R & \xrightarrow{\mathtt{pr}_1 \restriction_R} & Z \\ {\scriptstyle z}\downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle z} \\ F(Z) & \xleftarrow[F(\mathtt{pr}_0 \restriction_R)]{} & F(R) & \xrightarrow[F(\mathtt{pr}_1 \restriction_R)]{} & F(Z) \end{array} \,. \tag{2.2}$$

Le diagramme ci-dessus indique que $\mathtt{pr}_0 \restriction_R$ et $\mathtt{pr}_1 \restriction_R$ sont deux morphismes de F-coalgèbres. Si (Z, z) est une F-coalgèbre finale, la propriété universelle de celle-ci permet de conclure, par unicité, qu'on a $\mathtt{pr}_0 \restriction_R = \mathtt{pr}_1 \restriction_R$. On obtient donc le principe suivant.

Théorème 2.7 (Principe de coinduction)**.** *Soit (Z, z) une F-coalgèbre finale dans $\mathcal{Ens}$ et soit $x, y \in Z$. S'il existe une bisimulation $R \subseteq Z \times Z$ telle que $(x, y) \in R$, alors $x = y$.*

Démonstration. En utilisant l'équation $\mathtt{pr}_0 \restriction_R = \mathtt{pr}_1 \restriction_R$ et puisque $(x, y) \in R$, on trouve : $x = \mathtt{pr}_0(x, y) = \mathtt{pr}_1(x, y) = y$. □

Exemple 3. La relation d'égalité sur Z est (trivialement) toujours une bisimulation. Le principe de coinduction indique simplement que toutes les autres bisimulations sont contenues dans celle-ci. ■

Exemple 4. Considérons de nouveau la F-coalgèbre finale $A^\omega \xrightarrow{\langle \mathtt{Head}, \mathtt{Tail} \rangle} A \times A^\omega$ de l'Exemple 1. Le but de cet exemple est de caractériser les bisimulations sur A^ω.

Soit $\approx$ une bisimulation sur A^ω et soit γ sa structure, dont on dénote les images comme suit :

$$\gamma(\alpha, \beta) = (h_{\alpha\beta}, \alpha', \beta').$$

Pour tout $\alpha, \beta \in A^\omega$ tels que $\alpha \approx \beta$, le diagramme (2.2) signifie qu'on a les égalités suivantes :

$$(\mathtt{Head}(\alpha), \mathtt{Tail}(\alpha)) = (h_{\alpha\beta}, \alpha') \qquad , \qquad (\mathtt{Head}(\beta), \mathtt{Tail}(\beta)) = (h_{\alpha\beta}, \beta').$$

Or, cela implique $\mathtt{Head}(\alpha) = \mathtt{Head}(\beta)$, $\mathtt{Tail}(\alpha) = \alpha'$ et $\mathtt{Tail}(\beta) = \beta'$. Mais puisque le codomaine de γ est $F(\approx)$, on peut conclure $\mathtt{Tail}(\alpha) \approx \mathtt{Tail}(\beta)$.

Réciproquement soit $\approx$ une relation sur A^ω telle que pour tout $\alpha, \beta \in A^\omega$,

$$\alpha \approx \beta \quad \Rightarrow \quad \begin{cases} \texttt{Head}(\alpha) = \texttt{Head}(\beta) \\ \texttt{Tail}(\alpha) \approx \texttt{Tail}(\beta) \end{cases} . \tag{2.3}$$

Alors en définissant la structure $\gamma(\alpha, \beta) = (\texttt{Head}(\alpha), \texttt{Tail}(\alpha), \texttt{Tail}(\beta))$ sur $\approx$, on obtient une bisimulation sur A^ω.

Ainsi, pour démontrer *par coinduction* que deux mots $\alpha, \beta \in A^\omega$ sont égaux, il suffit de trouver une relation $\approx$ satisfaisant (2.3) et de démontrer $\alpha \approx \beta$. Philosophiquement, la stratégie d'une preuve par coinduction est donc de repousser le problème de démontrer l'égalité à plus tard (vers la queue du mot), contrairement à la stratégie de l'induction, qui consiste plutôt à ramener le problème vers les situations de base. ■

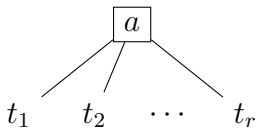
Exemple 5. On veut représenter les arbres possiblement infinis mais à branchements finis, dont les sommets sont étiquetés par un alphabet A. Soit $\mathcal{T}_A$ l'ensemble de ces arbres. Alors un arbre $t \in \mathcal{T}_A$ est complètement déterminé par l'étiquette $\texttt{Lab}(t)$ de sa racine ainsi que la liste (finie) $\texttt{Fils}(t)$ des sous-arbres de celle-ci. On a donc une structure de coalgèbre du foncteur $F(X) = A \times X^*$:

$$\langle \texttt{Lab}, \texttt{Fils} \rangle : \mathcal{T}_A \to A \times \mathcal{T}_A^* .$$

Puisque les branches infinies sont admises, alors de façon analogue à l'exemple de A^ω, $\mathcal{T}_A$ est le support de la F-coalgèbre finale. Sa structure est donc inversible, son inverse étant la fonction suivante :

$$\texttt{Cons} : A \times \mathcal{T}_A^* \to \mathcal{T}_A$$

$$\langle a, [t_1, t_2 \dots t_r] \rangle \mapsto$$



.

De quoi peut avoir l'air une bisimulation sur $\mathcal{T}_A$? Par un calcul semblable à celui de l'Exemple 4, il s'agit d'une relation $\approx$ telle que $\forall x, y \in \mathcal{T}_A$:

$$x \approx y \quad \Rightarrow \quad \begin{cases} \texttt{Lab}(x) = \texttt{Lab}(y) \\ \texttt{Fils}(x) \approx^* \texttt{Fils}(y) \end{cases} ,$$

où $\approx^*$ est la relation sur $\mathcal{T}_A^* =_\mu 1 + \mathcal{T}_A \times \mathcal{T}_A^*$ définie récursivement comme suit :

$$\varepsilon \approx^* \varepsilon \,,$$
$$s{:}u \approx^* t{:}v \iff s \approx t \text{ et } u \approx^* v \,.$$

En d'autres mots, si $x = \texttt{Cons}\langle a, [s_1 \dots s_m]\rangle$ et $y = \texttt{Cons}\langle b, [t_1 \dots t_n]\rangle$, alors $x \approx y$ doit impliquer les relations suivantes :

$$a = b \quad , \quad m = n \quad , \quad \forall i, s_i \approx t_i \,. \qquad \blacksquare$$

2.4 Systèmes dirigés d'équations

L'exemple 5 de la section précédente n'en était pas un de structure *purement* coinductive, puisque le foncteur F dépendait d'une définition de X^*, laquelle est plutôt inductive. On peut toutefois représenter $\mathcal{T}_A$ comme une solution, en la variable T, du système à deux équations et deux inconnues suivant :

$$\left\{ \begin{array}{lll} T & =_\nu & A \times L \\ L & =_\mu & \mathbf{1} + (T \times L) \end{array} \right\} . \tag{2.4}$$

Dans cette section, on étudie comment on peut représenter des objets par de tels systèmes, auxquels on ajoute une notion de *priorité* pour imposer l'unicité de leur solution.

Étant donné un ensemble fixé $\mathbb{V}$ de variables propositionnelles, l'ensemble $\mathfrak{F}$ des formules admissibles du côté droit d'un tel système est le plus petit ensemble

contenant $\mathbb{V} \cup \{0,1\}$ et tel que pour tout $\varphi_0, \varphi_1 \in \mathfrak{F}$, on a $(\varphi_0 + \varphi_1) \in \mathfrak{F}$ et $(\varphi_0 \times \varphi_1) \in \mathfrak{F}$. L'ensemble des sous-formules apparaissant dans une formule φ sera dénoté $\mathsf{SF}(\varphi)$, et celui des variables y apparaissant sera dénoté $\mathsf{VAR}(\varphi)$.

Étant donné une catégorie bicartésienne $\mathcal{C}$ quelconque, on peut interpréter les formules comme des foncteurs. En effet, soit V un sous-ensemble fini de $\mathbb{V}$. On dénote par $\mathfrak{F}_V$ l'ensemble des formules $\varphi \in \mathfrak{F}$ telles que $\mathsf{VAR}(\varphi) \subseteq V$. Soit $\varphi \in \mathfrak{F}_V$ et $\mathcal{C}^V = \prod_{X \in V} \mathcal{C}$. On définit l'***interprétation*** $[\varphi]_V$ de φ dans la catégorie bicartésienne $\mathcal{C}_V := \mathcal{F}un(\mathcal{C}^V, \mathcal{C})$ comme suit :

– si $\varphi = X \in V$, alors $[\varphi]_V = \mathtt{pr}^V_X$;
– si $\varphi = 0$ (resp. $\varphi = 1$), alors $[\varphi]_V = \mathbf{0}$ (resp. $[\varphi]_V = \mathbf{1}$) ;
– if $\varphi = (\varphi_0 + \varphi_1)$ (resp. $\varphi = (\varphi_0 \times \varphi_1)$), alors $[\varphi]_V = [\varphi_0]_V + [\varphi_1]_V$ (resp. $[\varphi_0]_V \times [\varphi_1]_V$).

Il faut noter que cette définition ne dépend de V que dans la mesure où celui-ci doit être assez gros pour contenir $\mathsf{VAR}(\varphi)$. Une simple induction montre, en effet, que si $V \subseteq W$, alors $[\varphi]_W = [\varphi]_V \circ \mathtt{pr}^W_V$, où $\mathtt{pr}^W_V : \mathcal{C}^W \to \mathcal{C}^V$ est le foncteur de projection. De plus, puisque le produit et le coproduit sont associatifs (à isomorphisme près) dans n'importe quelle catégorie bicartésienne, on se permettra d'éviter les parenthèses superflues et d'utiliser les notations compactes $\prod_{i \in I} \varphi_i$ et $\coprod_{i \in I} \varphi_i$ (pour un ensemble I fini) pour dénoter respectivement le produit et le coproduit indicé par I, sachant que l'interprétation des formules en sera inchangée.

Un ***système dirigé d'équations*** est un triplet $\mathcal{S} = \langle B, F, p \rangle$, où B est un sous-ensemble fini de $\mathbb{V}$ et $F : B \to \mathfrak{F}$, $p : B \to \mathbb{N}$ sont deux fonctions appelées respectivement « ***formule associée*** » et « ***priorité*** ». L'***équation associée*** à une variable $X \in B$ s'écrit « $X =_{p_X} F_X$ ». Les éléments de B sont appelés ***variables liées*** du système, et on dénotera plutôt B par $\mathsf{BV}(\mathcal{S})$ par la suite. On définit aussi les ensembles suivants :

– ***Sous-formules de $\mathcal{S}$:*** $\mathsf{SF}(\mathcal{S}) = \bigcup_{X \in \mathsf{BV}(\mathcal{S})} \mathsf{SF}(F_X)$;
– ***Variables de $\mathcal{S}$:*** $\mathsf{VAR}(\mathcal{S}) = \bigcup_{X \in \mathsf{BV}(\mathcal{S})} \mathsf{VAR}(F_X)$;
– ***Variables libres de $\mathcal{S}$:*** $\mathsf{FV}(\mathcal{S}) = \mathsf{VAR}(\mathcal{S}) \setminus \mathsf{BV}(\mathcal{S})$.

On dira que $\mathcal{S}$ est ***clos*** si $\mathsf{FV}(\mathcal{S}) = \varnothing$. On veut résoudre les équations associées à un système $\mathcal{S}$, c'est-à-dire, pour chaque $X \in \mathsf{BV}(\mathcal{S})$, interpréter X comme l'algèbre initiale (en la variable X) du foncteur $[F_X]_{\mathsf{VAR}(\mathcal{S})}$ si p_X est impair, ou comme la coalgèbre finale du même foncteur si p_X est pair.

Puisqu'on doit respecter la priorité des variables dans la résolution d'un système $\mathcal{S}$, on définit la solution par récurrence. Soit donc :

$$\mathsf{MAX}(\mathcal{S}) := \{X \in \mathsf{BV}(\mathcal{S}) \mid p_X \geq p_Y, \text{pour tout } Y \in \mathsf{BV}(\mathcal{S})\}.$$

Le ***système prédécesseur de $\mathcal{S}$*** est obtenu en retirant à $\mathcal{S}$ ses variables liées de priorité maximale, c'est-à-dire :

$$\mathsf{P}(\mathcal{S}) := \langle \mathsf{BV}(\mathcal{S}) \setminus \mathsf{MAX}(\mathcal{S}), F\restriction_{\mathsf{BV}(\mathcal{S})\setminus\mathsf{MAX}(\mathcal{S})}, p\restriction_{\mathsf{BV}(\mathcal{S})\setminus\mathsf{MAX}(\mathcal{S})} \rangle.$$

Définition. Soit $V \subseteq \mathbb{V}$ un ensemble fini tel que $\mathsf{FV}(\mathcal{S}) \subseteq V$ et $\mathsf{BV}(\mathcal{S}) \cap V = \varnothing$. La ***solution de $\mathcal{S}$*** est un foncteur $[\![\mathcal{S}]\!]_V : \mathcal{C}^V \to \mathcal{C}^{\mathsf{BV}(\mathcal{S})}$ défini comme suit :

– Si $\mathsf{BV}(\mathcal{S}) = \varnothing$, alors $\mathcal{C}^{\mathsf{BV}(\mathcal{S})} = \mathbb{1}$, où $\mathbb{1}$ est la catégorie terminale (avec un seul objet et sa flèche identité). On pose donc $[\![\mathcal{S}]\!]_V$ comme étant l'unique foncteur de $\mathcal{C}^V$ vers $\mathbb{1}$.
– Sinon, soit $V' = \mathsf{MAX}(\mathcal{S}) \cup V$. Alors on a $V' \cap \mathsf{BV}(\mathsf{P}(\mathcal{S})) = \varnothing$ et

$$\mathsf{FV}(\mathsf{P}(\mathcal{S})) \subseteq \mathsf{MAX}(\mathcal{S}) \cup \mathsf{FV}(\mathcal{S}) \subseteq \mathsf{MAX}(\mathcal{S}) \cup V = V'.$$

Donc, par récurrence, $[\![\mathsf{P}(\mathcal{S})]\!]_{V'} : \mathcal{C}^{V'} \to \mathcal{C}^{\mathsf{BV}(\mathsf{P}(\mathcal{S}))}$ est défini. Soit G et H les foncteurs suivants :

$$\begin{aligned} G &:= \langle [F_X]_{\mathsf{BV}(\mathcal{S})\cup V} \mid X \in \mathsf{MAX}(\mathcal{S}) \rangle : \mathcal{C}^{\mathsf{BV}(\mathcal{S})\cup V} \to \mathcal{C}^{\mathsf{MAX}(\mathcal{S})}, \\ H &:= \langle\, G\,,\ [\![\mathsf{P}(\mathcal{S})]\!]_{V'} \circ \mathtt{pr}_{V'}^{\mathsf{BV}(\mathcal{S})\cup V} \,\rangle : \\ &\quad \mathcal{C}^{\mathsf{BV}(\mathcal{S})\cup V} = \mathcal{C}^{\mathsf{BV}(\mathcal{S})} \times \mathcal{C}^V \longrightarrow \mathcal{C}^{\mathsf{MAX}(\mathcal{S})} \times \mathcal{C}^{\mathsf{BV}(\mathsf{P}(\mathcal{S}))} = \mathcal{C}^{\mathsf{BV}(\mathcal{S})}. \end{aligned} \tag{2.5}$$

Si $p(\mathsf{MAX}(S))$ est impair, soit $[\![\mathcal{S}]\!]_V$ l'algèbre initiale paramétrée du foncteur H ; sinon, $p(\mathsf{MAX}(\mathcal{S}))$ est pair et on pose $[\![\mathcal{S}]\!]_V$ comme la coalgèbre finale paramétrée du foncteur H.

Le lecteur pourrait objecter à la précédente définition qu'il existe des catégories pour lesquelles les algèbres initiales et coalgèbres finales considérées dans celle-ci n'existent pas. On concentrera notre attention sur les catégories dans lesquelles elles existent. De telles catégories sont dites μ-bicomplètes et on les définit plus précisément à la Section 2.6.

La solution d'un système $\mathcal{S}$ permet d'interpréter n'importe quelle formule $\varphi \in \mathfrak{F}_V$ par rapport à celle-ci. La ***signification*** de φ est le foncteur $[\![\varphi]\!]^{\mathcal{S}}_V : \mathcal{C}^V \to \mathcal{C}$ suivant :

$$[\![\varphi]\!]^{\mathcal{S}}_V = [\varphi]_{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathcal{S}]\!]_V, \mathtt{id} \rangle.$$

Lemme 2.8. *Pour toute formule φ définie sur un ensemble V de variables tel que $\mathsf{FV}(\mathcal{S}) \subseteq V$ et $V \cap \mathsf{BV}(\mathcal{S}) = \varnothing$, il existe un isomorphisme naturel*

$$\eta \ : \ [\![\varphi]\!]^{\mathcal{S}}_V \to [\![\varphi]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}, \mathtt{id}) \, ,$$

où $\vec{f}$ est le foncteur $\langle [\![X]\!]^{\mathcal{S}}_V \rangle_{X \in \mathsf{MAX}(\mathcal{S})}$. De plus, si $\varphi = X \in \mathsf{MAX}(\mathcal{S})$, cet isomorphisme est l'identité.

Démonstration. Par définition, on a, d'un côté,

$$[\![\varphi]\!]^{\mathcal{S}}_V = [\varphi]_{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathcal{S}]\!]_V, \mathtt{id} \rangle$$

et de l'autre côté,

$$\begin{aligned} [\![\varphi]\!]^{\mathsf{P}(\mathcal{S})}_{V\cup\mathsf{MAX}(\mathcal{S})}(\vec{f}, \mathtt{id}) &= [\varphi]_{\mathsf{BV}(\mathsf{P}(\mathcal{S}))\cup\mathsf{MAX}(\mathcal{S})\cup V} \circ \langle [\![\mathsf{P}(\mathcal{S})]\!]_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}, \mathtt{id}), \vec{f}, \mathtt{id} \rangle \\ &= [\varphi]_{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathsf{P}(\mathcal{S})]\!]_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}, \mathtt{id}), \vec{f}, \mathtt{id} \rangle \ . \end{aligned}$$

Il suffit donc de vérifier qu'on a un isomorphisme naturel

$$\widetilde{\eta} \ : \ [\![\mathcal{S}]\!]_V \to \langle [\![\mathsf{P}(\mathcal{S})]\!]_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}, \mathtt{id}), \vec{f}\rangle$$

Soit $V' = \mathsf{MAX}(\mathcal{S}) \cup V$. Puisque le codomaine de chacun de ces deux foncteurs est $\mathcal{C}^{\mathsf{BV}(X)}$, il suffit de vérifier que pour tout $X \in \mathsf{BV}(\mathcal{S})$, on a un isomorphisme naturel

$$\theta_X \ : \ \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ [\![\mathcal{S}]\!]_V \to \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ \langle [\![\mathsf{P}(\mathcal{S})]\!]_{V'}(\vec{f}, \mathtt{id}), \vec{f}\rangle \ .$$

– Si $X \in \mathsf{MAX}(\mathcal{S})$, alors on a

$$\begin{aligned}
\mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ \langle [\![\mathsf{P}(\mathcal{S})]\!]_{V'}(\vec{f}, \mathtt{id}), \vec{f}\rangle &= \mathtt{pr}_X^{\mathsf{MAX}(\mathcal{S})} \circ \vec{f} \\
&= [\![X]\!]_V^{\mathcal{S}} \\
&= [X]_{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \\
&= \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \\
&= \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ [\![\mathcal{S}]\!]_V \ .
\end{aligned}$$

  Il suffit donc de prendre $\theta_X = \mathtt{id}$. Cela conclut du même coup la deuxième partie de l'énoncé.

– Si $X \in \mathsf{BV}(\mathsf{P}(\mathcal{S}))$, soit $\tau : [\![\mathcal{S}]\!]_V \to H\big([\![\mathcal{S}]\!]_V, \mathtt{id}\big)$ un isomorphisme naturel (on sait qu'il en existe un par construction de $[\![\mathcal{S}]\!]_V$). Remarquons qu'on a

$$\begin{aligned}
\mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ \langle [\![\mathsf{P}(\mathcal{S})]\!]_{V'}(\vec{f}, \mathtt{id}), \vec{f}\rangle &= \mathtt{pr}_X^{\mathsf{BV}(\mathsf{P}(\mathcal{S}))} \circ [\![\mathsf{P}(\mathcal{S})]\!]_{V'}(\vec{f}, \mathtt{id}) \\
&= \mathtt{pr}_X^{\mathsf{BV}(\mathsf{P}(\mathcal{S}))} \circ [\![\mathsf{P}(\mathcal{S})]\!]_{V'} \circ \mathtt{pr}_{V'}^{\mathsf{BV}(\mathcal{S})}\big([\![\mathcal{S}]\!]_V, \mathtt{id}\big) \\
&= \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ H\big([\![S]\!]_V, \mathtt{id}\big) \ .
\end{aligned}$$

  Il suffit donc de prendre $\theta_X = \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ \tau$. □

Comme dans le cas de l'interprétation $[\varphi]_V$ des formules, la signification $[\![\varphi]\!]_V^{\mathcal{S}}$ ne dépend de V que dans le mesure où celui-ci est assez grand pour que la définition ait un sens. En effet, si $V \subseteq W$, une simple induction démontre $[\![\varphi]\!]_W^{\mathcal{S}} = [\![\varphi]\!]_V^{\mathcal{S}} \circ \mathtt{pr}_V^W$.

Pour cette raison, on omettra généralement d'indiquer l'ensemble V de variables sur lequel on définit la signification d'une formule, indiquant simplement $[\![\varphi]\!]^{\mathcal{S}}$. Par ailleurs, si le système d'équations $\mathcal{S}$ par rapport auquel on interprète la signification de φ est sous-entendu dans le contexte, on omettra également de l'indiquer, préférant la simple notation $[\![\varphi]\!]$.

Proposition 2.9. *Soit $\mathcal{S}$ un système dirigé d'équations et $X \in \mathsf{BV}(\mathcal{S})$. Si p_X est un nombre impair, alors il existe un isomorphisme naturel $\alpha_X : [\![F_X]\!] \to [\![X]\!]$. Si, au contraire, p_X est un nombre pair, alors il existe un isomorphisme naturel $\zeta_X : [\![X]\!] \to [\![F_X]\!]$.*

Démonstration. Fixons un ensemble V de variables tel qu'on ait $\mathsf{FV}(\mathcal{S}) \subseteq V$ et $V \cap \mathsf{BV}(\mathcal{S}) = \varnothing$. On procède par induction sur la priorité de $\mathsf{MAX}(\mathcal{S})$.

Soit $X \in \mathsf{MAX}(\mathcal{S})$. Alors par définition, on a :

$$\begin{aligned}[\![X]\!]_V &= [X]_{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \\ &= \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})\cup V} \circ \langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \\ &= \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ [\![\mathcal{S}]\!]_V .\end{aligned}$$

D'un autre côté, en se référant à l'équation (2.5), on trouve :

$$\begin{aligned}\mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})} \circ H\langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle &= \mathtt{pr}_X^{\mathsf{MAX}(\mathcal{S})} \circ G\langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \\ &= [F_X]_{\mathsf{BV}(\mathcal{S})\cup V}\langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \\ &= [\![F_X]\!]_V \ .\end{aligned}$$

Ainsi, si p_X est impair, alors $[\![\mathcal{S}]\!]_V$ est l'algèbre initiale paramétrée du foncteur H. Soit $\sigma : H\langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle \to [\![\mathcal{S}]\!]_V$ sa structure, qui est donc un isomorphisme naturel, et on pose :

$$\alpha_X := \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})}(\sigma) \ : \ [\![F_X]\!]_V \to [\![X]\!]_V \ .$$

De la même façon, si p_X est pair, alors $[\![\mathcal{S}]\!]_V$ est la coalgèbre finale paramétrée de H. Soit $\tau : [\![\mathcal{S}]\!]_V \to H\langle [\![\mathcal{S}]\!]_V, \mathtt{id}\rangle$ sa structure et on pose :

$$\zeta_X := \mathtt{pr}_X^{\mathsf{BV}(\mathcal{S})}(\tau) \ : \ [\![X]\!]_V \to [\![F_X]\!]_V \ .$$

On vient, du même coup, de démontrer le cas de base de l'induction, puisque dans celui-ci, on a $\mathsf{BV}(\mathcal{S}) = \mathsf{MAX}(\mathcal{S})$.

Soit maintenant $X \in \mathsf{BV}(\mathcal{S}) \setminus \mathsf{MAX}(\mathcal{S})$. Par le Lemme 2.8, il existe deux isomorphismes naturels :

$$\begin{aligned} \eta \ &: \ [\![X]\!]_V^{\mathcal{S}} \to [\![X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}, \mathtt{id}) \ ; \\ \xi \ &: \ [\![F_X]\!]_V^{\mathcal{S}} \to [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}, \mathtt{id}) \ , \end{aligned}$$

où $\vec{f}$ est le foncteur $\langle [\![Y]\!]_V^{\mathcal{S}}\rangle_{Y\in\mathsf{MAX}(\mathcal{S})}$.

Ainsi, si p_X est impair, alors par hypothèse d'induction, on peut trouver un isomorphisme naturel

$$\beta \ : \ [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V} \to [\![X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V} \ .$$

Il suffit alors de prendre $\alpha_X = (\theta_c)_{c\in\mathcal{C}^V}$ où θ_c est la composition suivante :

$$[\![F_X]\!]_V^{\mathcal{S}}(c) \xrightarrow{\xi_c} [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}(c), c) \xrightarrow{\beta_{\vec{f}(c),c}} [\![X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}(c), c) \xrightarrow{\eta_c^{-1}} [\![X]\!]_V^{\mathcal{S}}(c) \ .$$

Similairement, si p_X est pair, alors par hypothèse d'induction, on peut trouver un isomorphisme naturel

$$\gamma \ : \ [\![X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V} \to [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V} \ .$$

Il suffit alors de prendre $\zeta_X = (\theta_c)_{c\in\mathcal{C}^V}$ où θ_c est la composition suivante :

$$[\![X]\!]_V^{\mathcal{S}}(c) \xrightarrow{\eta_c} [\![X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}(c), c) \xrightarrow{\gamma_{\vec{f}(c),c}} [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}_{\mathsf{MAX}(\mathcal{S})\cup V}(\vec{f}(c), c) \xrightarrow{\xi_c^{-1}} [\![F_X]\!]_V^{\mathcal{S}}(c) \ .$$

□

2.5 Jeux de parité

Dans (Santocanale, 2002b), on trouve la description d'une solution canonique aux systèmes dirigés d'équations dans la catégorie des ensembles, que nous rappelons dans cette section. Cette solution fait appel à la théorie des jeux de parité, généralisée à partir des travaux de Joyal (1997) en y ajoutant des jeux *circulaires*. Rappelons d'abord de quoi il s'agit.

Un ***jeu de parité*** est un type particulier de jeux à deux joueurs, qu'on appellera σ et π. Formellement, il s'agit d'un triplet $J = \langle G, h, j\rangle$ où G est un graphe étiqueté déterministe (dont on se soucie peu de l'alphabet) et h, j sont deux fonctions appelées respectivement ***hauteur*** et ***joueur associé*** dont les types sont les suivants :

$$h : G \to \mathbb{N} \cup \{\infty\}$$
$$j : h^{-1}(\mathbb{N}) \to \{\sigma, \pi\}.$$

Étant donné une collection d'ensembles $E = \{E_v\}_{h(v)=\infty}$, les règles du jeu sont les suivantes. Au début de la partie, un jeton est placé sur un sommet $u_0 \in G$ tel que $h(u_0) < \infty$. Celui-ci détermine à qui le tour (σ ou π) selon la valeur de $j(u_0)$. Un tour, pour ce joueur, consiste simplement à choisir un successeur v de u_0 et déplacer le jeton sur celui-ci. S'il choisit un v tel que $h(v) = \infty$, le joueur choisit un élément de l'ensemble E_v et remporte aussitôt la partie. Si aucun mouvement n'est possible, il perd automatiquement. Autrement, un nouveau tour a lieu selon la nouvelle position du jeton (le joueur est déterminé par $j(v)$). Dans le cas où une partie est infinie, soit I l'ensemble des sommets sur lesquels le jeton s'est retrouvé une infinité de fois au cours de celle-ci et soit $m = \max(h(I))$. Si m est un nombre pair, on décrète que σ remporte la partie. Sinon, m est un nombre impair et on décrète que c'est π qui l'emporte.

Une partie est donc déterminée par une paire (γ, x) où γ est un chemin dans le graphe G et x est un choix d'élément de l'ensemble $E_{\varsigma_\gamma u_0}$ si γ est fini et $h(\varsigma_\gamma u_0) = \infty$ (sinon, on pose $x = \perp$). Une ***stratégie gagnante déterministe*** pour le joueur σ est un ensemble S de parties gagnantes pour σ tel que, pour tout $(\gamma, x) \in S$ et tout chemin fini $\beta \sqsubset \gamma$, la propriété suivante est satisfaite. Soit $u = \varsigma_\beta u_0$:

– si $j(u) = \pi$, alors *pour tout* symbole a pour lequel il existe $v \in G$ tel que $u \xrightarrow{a} v$, on peut trouver $(\gamma', x') \in S$ tel que $\beta \cdot a \sqsubseteq \gamma'$.
– si $j(u) = \sigma$, alors il existe *au plus un* symbole a pour lequel il existe $v \in G$ et $(\gamma', x') \in S$ tels que $u \xrightarrow{a} v$ et $\beta \cdot a \sqsubseteq \gamma'$.

En d'autres mots, une stratégie gagnante déterministe pour σ est un ensemble de parties gagnantes qui prévoit une et une seule riposte à chaque coup possible de π. On dénote par $W_G(E)$ l'ensemble des stratégies gagnantes pour σ dans le jeu G avec la collection d'ensembles E.

Revenons maintenant aux systèmes dirigés d'équations. Soit $\mathcal{S}$ un tel système dont on suppose, sans perte de généralité, que pour tout $X \in \mathsf{BV}(\mathcal{S})$, F_X est de la forme $\prod_{i\in I} X_i$ ou $\coprod_{i\in I} X_i$ pour I fini et $X_i \in \mathsf{VAR}(\mathcal{S}) \cup \{0, 1\}$. On définit le jeu de parité $J(\mathcal{S}) := \langle G, h, j\rangle$ comme suit :

– le support du graphe G est $\mathsf{VAR}(\mathcal{S}) \cup \{0, 1\}$ et il y a une transition $X \to Y$ si et seulement si $X \in \mathsf{BV}(\mathcal{S})$ et Y est une sous-formule de F_X ;
– on pose $h(0) = h(1) = 0$, $h(X) = p_X$ si $X \in \mathsf{BV}(\mathcal{S})$ et $h(X) = \infty$ autrement ;
– on pose $j(0) = \sigma$, $j(1) = \pi$ et, pour $X \in \mathsf{BV}(\mathcal{S})$, $j(X) = \sigma$ si $F_X = \coprod_{i\in I} X_i$, et $j(X) = \pi$ si $F_X = \prod_{i\in I} X_i$.

Prenons comme exemple le système d'équations (2.4), légèrement remanié en un système dirigé $\mathcal{S}$ (avec les priorités) tel que chaque membre de droite ait un seul connecteur ($+$ ou $\times$). La Figure 2.2 montre la conversion de $\mathcal{S}$ en le jeu $J(\mathcal{S})$. La hauteur des sommets est indiquée par les boîtes en pointillé et les joueurs associés

sont identifiés par les types de noeuds ($\oplus$ pour σ et $\otimes$ pour π).

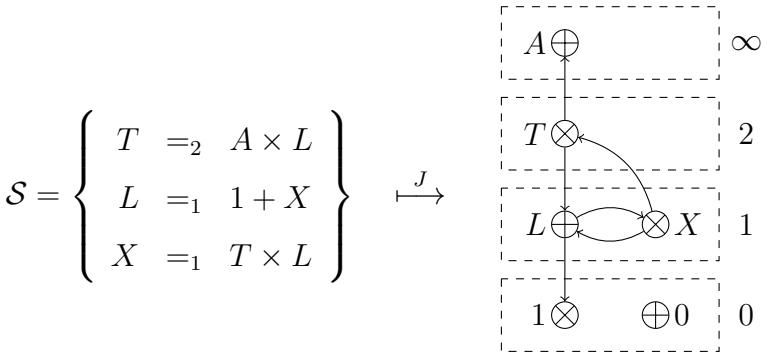


Figure 2.2 Un système dirigé $\mathcal{S}$ et le jeu $J(\mathcal{S})$ associé

Comment décrire une stratégie gagnante dans cet exemple, à partir de la position de départ T ? Il faut préparer un symbole $a \in A$ pour le cas où π jouerait vers la position A, et une stratégie gagnante à partir de L pour l'autre situation. Une telle stratégie peut consister soit en un mouvement vers la position 1 (auquel cas la partie est remportée), ou bien vers la position X, auquel cas il faut prévoir deux ripostes (une stratégie à partir de T et une à partir de L) selon le choix de π. Puisque $h(X)$ est pair, on peut se permettre un nombre infini de passages par T dans la stratégie, mais pas un nombre infini de passages par L sans d'abord revenir par T (puisque $h(L)$ est impair).

On peut encoder une stratégie gagnante pour σ par un arbre t possiblement infini mais à branchements finis, muni d'un étiquetage $\lambda : t \to A$ des sommets. En effet, à la racine de t, $\lambda(a)$ encode le symbole qu'on choisit si π déplace le jeton vers A, et l'autre riposte est constituée d'un nombre fini d'aller-retours entre L et X où, chaque fois, on doit prévoir un nouvelle stratégie à partir de T (un nouvel arbre). Chaque aller-retour encode un des sous-arbres à partir de la racine. On peut donc dire que $W_{J(\mathcal{S})}(A) \cdot \mathtt{pr}_T$ est isomorphe à $\mathcal{T}_A$. Cela relève d'un résultat plus général, qui est le théorème principal de (Santocanale, 2002b).

Théorème 2.10 (Santocanale, 2002b, Th. 5.4)**.** $[\![\mathcal{S}]\!](E) \cong W_{J(\mathcal{S})}(E)$.

Le dernier exemple indique, au passage, l'importance de la priorité dans un système dirigé d'équations (et pas seulement celle de la parité de celle-ci). En effet, supposons qu'on change les priorités sans changer leur parité, pour obtenir le nouveau système suivant :

$$\mathcal{S}' = \left\{ \begin{array}{lll} T & =_2 & A \times L \\ L & =_3 & 1 + X \\ X & =_1 & T \times L \end{array} \right\} .$$

Alors dans le jeu $J(\mathcal{S}')$, il n'est plus autorisé de passer un nombre infini de fois par le sommet T, puisque pour le faire, il faut aussi passer une infinité de fois par le sommet L. Mais puisque p_L est impair et $p_L > p_T$, alors une telle partie donnerait la victoire au joueur π. $[\![T]\!]^{\mathcal{S}'}(A)$ est donc maintenant l'ensemble des arbres *finis* étiquetés par A.

Toutefois, dans les cas où la parité de la priorité sera la seule valeur importante dans un système dirigé donné, on se permettra de dénoter les équations « $X =_\mu F_X$ » ou « $X =_\nu F_X$ », selon le cas.

2.6 Catégories μ-bicomplètes

En terminant ce chapitre, il importe de préciser l'hypothèse qu'on a faite, à la Section 2.4, sur une catégorie $\mathcal{C}$ pour affirmer qu'on pouvait y interpréter les systèmes dirigés d'équations, à savoir, que $\mathcal{C}$ soit une catégorie μ-bicomplète. Il s'agit d'une condition plus faible que la bicomplétude (Joyal, 1995), qui consiste en l'existence de toutes les limites et colimites, car elles est restreinte aux limites et colimites issues des algèbres initiales et coalgèbres finales. On reprend la définition des catégories μ-bicomplètes que l'on peut trouver dans Santocanale (2002b).

Définition. L'ensemble $\mu\mathcal{T}$ des ***μ-termes*** est le plus petit ensemble contenant $\mathbb{V} \cup \{0, 1\}$ et tel que :

– si $t_0, t_1 \in \mu\mathcal{T}$, alors $(t_0 + t_1) \in \mu\mathcal{T}$ et $(t_0 \times t_1) \in \mu\mathcal{T}$;
– si $t \in \mu\mathcal{T}$ et $X \in \mathbb{V}$, alors $\mu X.t \in \mu\mathcal{T}$ et $\nu X.t \in \mu\mathcal{T}$.

Étant donné un μ-terme t, l'ensemble de ses variables, dénoté $\mathsf{FV}(t) \subset \mathbb{V}$, est défini comme suit :

– si $t = 0$ ou $t = 1$, alors $\mathsf{FV}(t) = \varnothing$;
– si $t = X \in \mathbb{V}$, alors $\mathsf{FV}(t) = \{X\}$;
– si $t = (t_0 + t_1)$ ou $t = (t_0 \times t_1)$, alors $\mathsf{FV}(t) = \mathsf{FV}(t_0) \cup \mathsf{FV}(t_1)$;
– si $t = \mu X.t'$ ou $t = \nu X.t'$, alors $\mathsf{FV}(t) = \mathsf{FV}(t') \setminus \{X\}$.

Un μ-terme t est ***clos*** si $\mathsf{FV}(t) = \varnothing$. Étant donné $s, t \in \mu\mathcal{T}$ et $X \in \mathbb{V}$ on peut construire le terme $s[X/t]$ de façon usuelle, en remplaçant chaque occurrence de X dans s qui n'est pas capturée par un quantificateur (μ ou ν) par le terme t.

Définition. Soit $\mathcal{C}$ une catégorie bicartésienne. Pour tout $t \in \mu\mathcal{T}$, soit V un ensemble fini tel que $\mathsf{FV}(t) \subseteq V \subset \mathbb{V}$. L'***interprétation*** de t dans $\mathcal{C}$ par rapport au contexte V est le foncteur $\|t\|_V : \mathcal{C}^V \to \mathcal{C}$ défini comme suit :

– si $t = 0$, alors $\|t\|_V \equiv \mathbf{0}$;
– si $t = 1$, alors $\|t\|_V \equiv \mathbf{1}$;
– si $t = X \in V$, alors $\|t\|_V = \mathtt{pr}^V_X$;
– si $t = (t_0 + t_1)$, alors $\|t\|_V = \|t_0\|_V + \|t_1\|_V$;
– si $t = (t_0 \times t_1)$, alors $\|t\|_V = \|t_0\|_V \times \|t_1\|_V$;
– si $t = \mu X.t'$ et $X \notin V$, alors $\|t\|_V$ est l'algèbre initiale paramétrée du foncteur $\|t'\|_{\{X\}\cup V} : \mathcal{C} \times \mathcal{C}^V \to \mathcal{C}$;
– si $t = \nu X.t'$ et $X \notin V$, alors $\|t\|_V$ est la coalgèbre finale paramétrée du foncteur $\|t'\|_{\{X\}\cup V} : \mathcal{C} \times \mathcal{C}^V \to \mathcal{C}$.

La catégorie $\mathcal{C}$ est ***μ-bicomplète*** si elle est localement petite et si, pour chaque μ-terme t et $V \subset \mathbb{V}$ satisfaisant les conditions ci-dessus, le foncteur $\|t\|_V$ est bien défini.

Des exemples de catégories μ-bicomplètes incluent, bien sûr, la catégorie des en-

sembles ainsi que les treillis complets, mais aussi des structures plus générales telles que les μ-treillis (Santocanale, 2000) et les catégories localement présentables, notamment les catégories de préfaisceaux et de faisceaux (Santocanale, 2002b).

Proposition 2.11. *Soit $\mathcal{C}$ une catégorie μ-bicomplète. Alors, pour tout système dirigé $\mathcal{S}$ et tout ensemble fini $V \subseteq \mathbb{V}$ tel que $\mathsf{FV}(\mathcal{S}) \subseteq V$ et $\mathsf{BV}(\mathcal{S}) \cap V = \varnothing$, le foncteur $[\![\mathcal{S}]\!]_V : \mathcal{C}^V \to \mathcal{C}^{\mathsf{BV}(\mathcal{S})}$ est bien défini.*

Démonstration. Si $\mathsf{BV}(\mathcal{S}) = 0$, le foncteur $[\![\mathcal{S}]\!]_V : \mathcal{C}^V \to \mathbb{1}$ est bien défini, peu importe la catégorie $\mathcal{C}$. Du reste, la définition de $[\![\mathcal{S}]\!]_V$ est faite par récurrence en n'utilisant aucun autre constructeur que $\mathbf{0}$, $\mathbf{1}$, $+$, $\times$, les algèbres initiales paramétrées et les coalgèbres finales paramétrées. Tous ces outils sont disponibles dans $\mathcal{C}$ sur des foncteurs ainsi récursivement définis. □

La réciproque de la proposition précédente est également vraie (voir la Proposition 2.12 ci-dessous). On aurait donc plus prendre, comme définition alternative des catégories μ-bicomplètes, que ce sont les catégories qui permettent d'interpréter les systèmes dirigés d'équations.

Proposition 2.12. *Soit $\mathcal{C}$ une catégorie μ-bicomplète. Alors, pour tout terme $t \in \mu\mathcal{T}$, il existe une formule φ_t et un système dirigé d'équations $\mathcal{S}_t$ tel que $\|t\|_V = [\![\varphi_t]\!]_V^{\mathcal{S}_t}$. De plus, si s est un sous-terme de t, alors on peut choisir $\mathcal{S}_s$ et $\mathcal{S}_t$ de façon à avoir $\mathcal{S}_s \subseteq \mathcal{S}_t$.*

Démonstration. On procède par induction sur t. Supposons d'abord, sans perte de généralité, que pour toute variable $X \in \mathbb{V}$, si X a une occurrence dans t, alors ou bien toutes ces occurrences sont libres, ou bien elles sont toutes liées par un même quantificateur.

Alors, si $t \in \{0,1\} \cup \mathbb{V}$, il suffit de prendre $\varphi_t = t$ et $\mathcal{S}_t$ est le système vide (qui n'a aucune variable liée). Si $t = (t_0 + t_1)$ (resp. $t = (t_0 \times t_1)$), il suffit de prendre $\varphi_t = (\varphi_{t_0} + \varphi_{t_1})$ (resp. $\varphi_t = (\varphi_{t_0} \times \varphi_{t_1})$) et $\mathcal{S}_t = \mathcal{S}_{t_0} \cup \mathcal{S}_{t_1}$.

Enfin, si $t = \mu X.t'$ (resp. $t = \nu X.t'$) et $\mathcal{S}_{t'} = \langle B, F, p\rangle$, on pose $\varphi_t = X$ et $\mathcal{S}_t = \langle B \cup \{X\}, F', p'\rangle$ où $F_Y = F'_Y$ et $p_Y = p'_Y$ pour tout $Y \in B$ et où $F'_X = \varphi_{t'}$ et p'_X est le plus petit nombre naturel n impair (resp. pair) tel que $n \geq p_{\mathsf{MAX}(\mathcal{S}_{t'})}$.

Remarquons que cette construction ne peut que faire grandir le système d'équations associé à un terme, en fonction de la profondeur de celui-ci. Autrement dit, si s est un sous-terme de t, alors on a $\mathcal{S}_s \subseteq \mathcal{S}_t$. □

Exemple 1. Soit $t = \nu T.(\nu X.(1 + X) \times \mu L.(1 + (T \times L)))$. Alors la conversion de t en système dirigé d'équations va comme suit :

$$\mathcal{S}_t = \left\{ \begin{array}{l} T =_2 X \times L \\ X =_2 1 + X \\ L =_1 1 + (T \times L) \end{array} \right\}.$$

Réciproquement, étant donné le système $\mathcal{S}_t$, on peut retrouver le terme original t en *imbriquant* les équations les unes dans les autres. La priorité indique la nature et l'ordre des quantificateurs μX et νX. Les systèmes dirigés d'équations ne sont donc qu'une syntaxe alternative à celle des μ-termes. ■

Définition. Soit $\mathcal{C}$, $\mathcal{D}$ deux catégories μ-bicomplètes. Pour chaque $t \in \mu\mathcal{T}$, on dénote par $\|t\|^{\mathcal{C}}_V$ et $\|t\|^{\mathcal{D}}_V$ l'interprétation fonctorielle de t dans $\mathcal{C}$ et $\mathcal{D}$ respectivement. Un ***morphisme*** de catégories μ-bicomplètes (entre $\mathcal{C}$ et $\mathcal{D}$) est un foncteur $F : \mathcal{C} \to \mathcal{D}$ tel que, pour tout $t \in \mu\mathcal{T}$, le diagramme suivant commute :

$$\begin{array}{ccc} \mathcal{C}^V & \xrightarrow{F^V} & \mathcal{D}^V \\ {\scriptstyle \|t\|^{\mathcal{C}}_V}\downarrow & & \downarrow{\scriptstyle \|t\|^{\mathcal{D}}_V} \\ \mathcal{C} & \xrightarrow{F} & \mathcal{D} \end{array}.$$

Il convient d'insister sur une famille particulière de catégories μ-bicomplètes, qui sera en vedette à la Section 4.3. Il s'agit des *catégories μ-bicomplètes libres*. Essentiellement, il s'agit de catégories μ-bicomplètes $\mathcal{M}(B)$, où B est un ensemble de générateurs, qui ne dispose d'aucune structure supplémentaire à ce qui est imposé par les axiomes. La construction qu'on en donne est assez standard en algèbre universelle et s'apparente à celle d'un groupe libre ou encore d'un espace vectoriel engendré par une base.

On définit d'abord un graphe étiqueté, $\mu\mathcal{G}_0$, dont les sommets sont les μ-termes et dont les arêtes sont les suivantes, pour chaque $t \in \mu\mathcal{T}$:
– $t \xrightarrow{\mathtt{id}_t} t$, $0 \xrightarrow{?_t} t$ et $t \xrightarrow{!_t} 1$;
– si $t = (t_0 + t_1)$, alors $t_0 \xrightarrow{\mathtt{in}_0} t$ et $t_1 \xrightarrow{\mathtt{in}_1} t$;
– si $t = (t_0 \times t_1)$, alors $t \xrightarrow{\mathtt{pr}_0} t_0$ et $t \xrightarrow{\mathtt{pr}_1} t_1$;
– si $t = \mu X.t'$, alors $t'[X/t] \xrightarrow{\alpha_t} t$;
– si $t = \nu X.t'$, alors $t \xrightarrow{\zeta_t} t'[X/t]$.
Soit ensuite $\mu\mathcal{G}$ le plus petit graphe contenant $\mu\mathcal{G}_0$ et tel que les propriétés suivantes sont vérifiées (chacune est quantifiée universellement sur les arêtes de $\mu\mathcal{G}$) :
– si $r \xrightarrow{f} s$ et $s \xrightarrow{g} t$, alors $r \xrightarrow{f \cdot g} t$;
– si $s \xrightarrow{f} t_0$ et $s \xrightarrow{g} t_1$, alors $s \xrightarrow{\langle f,g \rangle} (t_0 \times t_1)$;
– si $s_0 \xrightarrow{f} t$ et $s_1 \xrightarrow{g} t$, alors $(s_0 + s_1) \xrightarrow{\{f,g\}} t$;
– si $t = \mu X.t'$ et $t'[X/s] \xrightarrow{f} s$, alors $t \xrightarrow{a^t_f} s$;
– si $t = \nu X.t'$ et $s \xrightarrow{f} t'[X/s]$, alors $s \xrightarrow{z^t_f} t$.
On a ainsi assez de flèches pour pouvoir tracer les diagrammes de produits, coproduits, algèbres initiales et coalgèbres finales dans $\mu\mathcal{G}$, mais pas encore assez de structure pour vérifier leur propriété universelle.

Définition. Soit $r \in \mu\mathcal{T}$, $X \in \mathbb{V}$ et $s \xrightarrow{f} t$ une arête de $\mu\mathcal{G}$. On définit l'arête $r[X/s] \xrightarrow{r[X/f]} r[X/t]$ par récurrence comme suit :
– si $r = X$, alors $r[X/f] = f$;

– si $r \in \{0,1\} \cup \mathbb{V}$ et $r \neq X$, alors $r[X/f] = \mathtt{id}_r$;
– si $r = (r_0 + r_1)$, alors $r[X/f] = \{r_0[X/f] \cdot \mathtt{in}_0\,,\, r_1[X/f] \cdot \mathtt{in}_1\}$;
– si $r = (r_0 \times r_1)$, alors $r[X/f] = \langle \mathtt{pr}_0 \cdot r_0[X/f]\,,\, \mathtt{pr}_1 \cdot r_1[X/f] \rangle$;
– si $r = \mu Y.r'$ où $Y \neq X$, alors $r[X/f] = a_g^{r(s)}$ où $g = r'[Y/r(t)][X/f] \cdot \alpha_{r(t)}$ et

$$r(u) = r[X/u] = \mu Y.r'[X/u] \qquad (u \in \{s,t\})\,;$$

– si $r = \nu Y.r'$ où $Y \neq X$, alors $r[X/f] = z_g^{r(s)}$ où $g = \zeta_{r(t)} \cdot r'[Y/r(t)][X/f]$.

Une ***congruence*** est une relation d'équivalence $\sim$ sur les arêtes de $\mu\mathcal{G}$ qui satisfait les propriétés supplémentaires suivantes.

Axiomes des catégories :
– $\forall (s \xrightarrow{f} t)$, on a $\mathtt{id}_s \cdot f \sim f$ et $f \sim f \cdot \mathtt{id}_t$;
– $\forall (r \xrightarrow{f} s), (s \xrightarrow{g} t), (t \xrightarrow{h} u)$, on a $(f \cdot g) \cdot h \sim f \cdot (g \cdot h)$.
Axiomes des produits :
– $\forall (s \xrightarrow{f} t_0), (s \xrightarrow{g} t_1)$, on a $\langle f, g \rangle \cdot \mathtt{pr}_0 \sim f$ et $\langle f, g \rangle \cdot \mathtt{pr}_1 \sim g$;
– $\forall (s \xrightarrow{f} t_0), (s \xrightarrow{g} t_1), (s \xrightarrow{p} t_0 \times t_1)$, si $p \cdot \mathtt{pr}_0 \sim f$ et $p \cdot \mathtt{pr}_1 \sim g$, alors $p \sim \langle f, g \rangle$.
Axiomes des coproduits :
– $\forall (s_0 \xrightarrow{f} t), (s_1 \xrightarrow{g} t)$, on a $\mathtt{in}_0 \cdot \{f, g\} \sim f$ et $\mathtt{in}_1 \cdot \{f, g\} \sim g$;
– $\forall (s_0 \xrightarrow{f} t), (s_1 \xrightarrow{g} t), (s_0 + s_1 \xrightarrow{q} t)$, si $\mathtt{in}_0 \cdot q \sim f$ et $\mathtt{in}_1 \cdot q \sim g$, alors $q \sim \{f, g\}$.
Axiomes des algèbres initiales : (où $t = \mu X.t'$)
– $\forall (t'[X/s] \xrightarrow{f} s)$, on a $\alpha_t \cdot a_f^t \sim t'[X/a_f^t] \cdot f$;
– $\forall (t'[X/s] \xrightarrow{f} s), (t \xrightarrow{g} s)$, si $\alpha_t \cdot g \sim t'[X/g] \cdot f$, alors $g \sim a_f^t$.
Axiomes des coalgèbres finales : (où $t = \nu X.t'$)
– $\forall (s \xrightarrow{f} t'[X/s])$, on a $z_f^t \cdot \zeta_t \sim f \cdot t'[X/z_f^t]$;
– $\forall (s \xrightarrow{f} t'[X/s]), (s \xrightarrow{g} t)$, si $g \cdot \zeta_t \sim f \cdot t'[X/g]$, alors $g \sim z_f^t$.
Par inspection des axiomes énumérés ci-dessus, un exemple trivial de congruence est la relation suivante :

$$(s \xrightarrow{f} t) \sim_\top (s' \xrightarrow{f'} t') \quad \Longleftrightarrow \quad s = s' \text{ et } t = t'\,.$$

De plus, étant donné une collection non vide $E = \{\sim_i : i \in I\}$ de congruences, la relation

$$f \sim^E g \quad \iff \quad \forall i \in I,\ f \sim_i g$$

est encore une congruence (c'est l'infimum de E). Il s'ensuit qu'il existe une congruence minimale, qu'on dénote $\sim_\perp$ (c'est l'infimum de la collection, non vide, de toutes les congruences). Soit enfin $\widetilde{\mu\mathcal{G}} = \mu\mathcal{G}/\sim_\perp$. On ne fera pas de différence typographique entre la classe d'équivalence d'un μ-terme t et le terme t lui-même.

Définition. Soit B un ensemble, dit de ***générateurs*** et $\lambda : B \to \mathbb{V}$ une fonction injective. On définit $\mathcal{M}(B)$ comme étant la catégorie dont les objets sont les $t \in \mu\mathcal{T}$ tels que $\mathsf{FV}(t) \subseteq \lambda(B)$ et dont les flèches sont les arêtes $s \xrightarrow{f} t$ de $\widetilde{\mu\mathcal{G}}$ telles que s et t sont des objets de $\mathcal{M}(B)$.

Proposition 2.13. *$\mathcal{M}(B)$ est une catégorie μ-bicomplète libre sur B.*

Démonstration. Le fait que $\mathcal{M}(B)$ est une catégorie est simplement dû au fait qu'on a inséré les axiomes des catégories dans la définition d'une congruence.

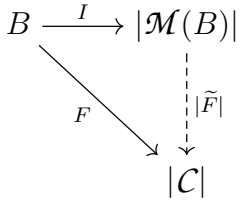
Pour montrer que $\mathcal{M}(B)$ est μ-bicomplète, il suffit de donner l'interprétation de chaque $t \in \mu\mathcal{T}$ en tant que foncteur $\|t\|_V : \mathcal{M}(B)^V \to \mathcal{M}(B)$. Soit $V = \{X_1 \dots X_n\}$ et on pose

$$\|t\|_V(x_1 \dots x_n) = t[X_1/x_1] \cdots [X_n/x_n]\,.$$

Le fait que $\|t\|_V$ est le foncteur recherché n'est que la conséquence de sa définition et du fait qu'on a inséré les axiomes de produits, coproduits, algèbres initiales et coalgèbres finales dans la définition d'une congruence.

Enfin, on doit montrer que $\mathcal{M}(B)$ est libre. Remarquons qu'on peut identifier l'ensemble B à la catégorie discrète dont les objets sont les éléments de B (avec aucune flèche sauf les identités). Soit $|\cdot|$ le foncteur oubliant (qui transforme une

catégorie μ-bicomplète en une simple catégorie). On veut donc construire un foncteur $I : B \to |\mathcal{M}(B)|$ (c'est-à-dire, simplement une fonction) tel que pour toute autre catégorie μ-bicomplète $\mathcal{C}$ et toute fonction $F : B \to |\mathcal{C}|$, il existe un unique morphisme de catégories μ-bicomplètes $\widetilde{F} : \mathcal{M}(B) \to \mathcal{C}$ tel que le diagramme suivant commute :



. (2.6)

Soit $B = \{b_1 \dots b_n\}$ et $V = \lambda(B) = \{X_1 \dots X_n\}$. Il suffit de prendre

$$I := B \xrightarrow{\lambda} V \hookrightarrow |\mathcal{M}(B)|\,.$$

Alors, étant donné une fonction $F : B \to |\mathcal{C}|$, on définit $\widetilde{F} : \mathcal{M}(B) \to \mathcal{C}$ sur les objets de $\mathcal{M}(B)$ par l'équation

$$\widetilde{F}(t) = \|t\|_V^{\mathcal{C}}(F(b_1) \dots F(b_n)).$$

La définition de $\widetilde{F}$ sur les flèches de $\mathcal{M}(B)$ se fait par récurrence sur les flèches de $\mu\mathcal{G}$, puisque $\sim_\perp$ est le plus petit point fixe de la définition de congruence avec, comme cas de base, les arêtes de $\mu\mathcal{G}_0$. On obtient ainsi un morphisme de catégories μ-bicomplètes faisant commuter le diagramme (2.6). □

Deuxième partie

Preuves circulaires

CHAPITRE III

SYNTAXE ET INTERPRÉTATION

Dans ce chapitre, on définit un système logique qui permet de construire des *preuves circulaires*, c'est-à-dire que celles-ci permettent de démontrer certaines formules par des raisonnements cycliques. Il s'agit d'une extension du système présenté dans Santocanale (2001), auquel on a ajouté la règle de coupure. La présentation faite dans ce chapitre ne se veut pas trop formelle et vise une interprétation des preuves circulaires comme dénotant des programmes dont les structures de données sont définies par un système dirigé d'équations. On élabore plus formellement, à la section 3.4, sur la *condition de garde*, qui assure la validité des preuves circulaires. Cette validité ne sera démontrée formellement qu'au Chapitre 4.

3.1 Logique et preuves

Une façon de résumer la logique mathématique est de dire qu'elle est l'étude des *formules*. Cela est très vague et prend évidemment plusieurs directions possibles dont l'une d'entre elles, la théorie de la démonstration, concerne les façons d'obtenir des formules à partir d'autres via des *règles d'inférence* et ce que cela signifie sémantiquement. Ce sujet est traité en détails dans (Girard, 2006) ou encore dans (David *et al.*, 2004) et on ne fait ici qu'en brosser un portrait très sommaire afin

d'établir des définitions appropriées pour nos besoins.

On suppose que l'ensemble $\mathfrak{F}$ des formules est donné d'avance (on pourrait prendre, par exemple, les formules du premier ordre, avec les symboles logiques habituels : $\vee$, $\wedge$, $\rightarrow$, $\neg$, $\forall$ et $\exists$). Un ***séquent simple*** est une expression formelle de la forme "$A \vdash B$", où $A, B \in \mathfrak{F}$. Le symbole $\vdash$ représente l'implication logique, à un niveau métalinguistique (dit *structurel*). Autrement dit, $A \vdash B$ n'est pas une formule et se lit « *La formule A entraîne logiquement la formule B* ». Les séquents simples sont les seuls qui seront considérés dans cette thèse, mais il faut savoir que la notion usuelle de *séquent* permet de placer plusieurs formules de chaque côté du symbole $\vdash$, modélisant ainsi la conjonction (à gauche) ou la disjonction (à droite) au niveau structurel. On dénote par $\mathsf{SEQ}_{\mathfrak{F}}$ l'ensemble des séquents sur $\mathfrak{F}$.

Une ***règle d'inférence*** est une expression de la forme

$$\frac{A_0 \vdash B_0 \quad A_1 \vdash B_1 \quad \ldots \quad A_{n-1} \vdash B_{n-1}}{A \vdash B}\,\texttt{Nom}$$

où `Nom` est un nom attribué de façon unique à la règle (de sorte qu'on puisse identifier les règles à leurs noms), n est l'***arité*** de la règle et les A_i, B_i, A, B sont des (schémas de) formules. Par exemple, voici les règles de la conjonction, tirées du système **LK** de Gentzen (voir Girard, 2006), dans le cas où les séquents sont simples (A, B et C peuvent être des formules quelconques).

$$\frac{A \vdash C}{A \wedge B \vdash C}\,\texttt{L}\wedge_0 \quad , \quad \frac{B \vdash C}{A \wedge B \vdash C}\,\texttt{L}\wedge_1 \quad , \quad \frac{A \vdash B \quad A \vdash C}{A \vdash B \wedge C}\,\texttt{R}\wedge \ .$$

La barre horizontale représente une implication logique d'encore un niveau métalinguistique par rapport au niveau structurel. Par exemple, la règle `R`$\wedge$ se lit comme suit : « *Si la formule A entraîne logiquement la formule B et si la formule A entraîne logiquement la formule C, alors la formule A entraîne logiquement la formule $B \wedge C$.* »

Un ***système déductif*** est une paire $\mathbf{S} = \langle \mathfrak{F}, \Sigma \rangle$ où $\mathfrak{F}$ est un ensemble de formules et Σ est une ***signature***, c'est-à-dire un ensemble de (noms de) règles d'inférence sur ces formules, avec une fonction d'arité $\mathrm{ar} : \Sigma \to \mathbb{N}$. Les règles d'inférence sont alors les briques qui composent les *preuves* du système.

Définition. Une ***preuve*** dans un système $\mathbf{S}$ est un triplet $\Pi = \langle G, \textsc{Règ}, \textsc{Seq} \rangle$ où G est un graphe étiqueté déterministe sur l'alphabet $\mathbb{N}$ et $\textsc{Règ} : G \to \Sigma$ et $\textsc{Seq} = (\textsc{Seq}_{\mathtt{L}} \vdash \textsc{Seq}_{\mathtt{R}}) : G \to \mathsf{SEQ}_{\mathfrak{F}}$ sont deux fonctions de sorte que pour chaque $u \in G$, les propriétés suivantes sont satisfaites :

1. $d := \deg(u) = \mathrm{ar}(\textsc{Règ}(u))$;
2. $\{a \in \mathbb{N} : \varsigma_a u \text{ est défini}\} = \{0, \dots d-1\}$;
3. l'expression suivante est une règle d'inférence du système :

$$\frac{\textsc{Seq}(\varsigma_0 u) \quad \dots \quad \textsc{Seq}(\varsigma_{d-1} u)}{\textsc{Seq}(u)}\, \textsc{Règ}(u).$$

Le graphe G s'appelle le ***support*** de Π et sera dénoté $|\Pi|$. On se permettra également un léger abus de langage en écrivant $u \in \Pi$ pour signifier $u \in G$. Enfin, on dit que Π est une *preuve de* $A \vdash B$ s'il existe $u \in \Pi$ tel que $\textsc{Seq}(u) = A \vdash B$.

Fait à remarquer sur cette définition : les preuves, pour nous, sont des *graphes quelconques* et non pas spécifiquement des arbres finis comme c'est généralement le cas dans les systèmes déductifs usuels. Cela ne change, en pratique, rien pour un système comme **LK** car les règles sont conçues de façon à ce que les chemins infinis soient impossibles à cause de la syntaxe des formules. Ce ne sera pas le cas dans le système qu'on étudiera dans cette thèse, d'où la possibilité des preuves circulaires.

Il s'agit des systèmes déductifs. Un système déductif $\mathbf{S}$ engendre une catégorie $\mathcal{S}$ dont les objets sont les formules et les flèches $f : A \to B$ sont *les preuves* du

séquent $A \vdash B$, pourvu que le système admette les deux règles suivantes :

$$\frac{}{A \xrightarrow{\mathrm{id}_A} A}\,\mathtt{I} \qquad , \qquad \frac{A \xrightarrow{f} C \quad C \xrightarrow{g} B}{A \xrightarrow{f\cdot g} B}\,\mathtt{C}\,.$$

La règle C s'appelle *syllogisme*, ou encore, *règle de coupure* en logique. Pour passer de **S** à $\mathcal{S}$, on doit identifier certaines (structures locales de) preuves de façon à satisfaire les axiomes des catégories, c'est-à-dire :

Associativité.

$$\frac{\dfrac{A \xrightarrow{f} C \quad C \xrightarrow{g} D}{A \xrightarrow{f\cdot g} D}\,\mathtt{C} \qquad D \xrightarrow{h} B}{A \xrightarrow{(f\cdot g)\cdot h} B}\,\mathtt{C} \quad = \quad \frac{A \xrightarrow{f} C \qquad \dfrac{C \xrightarrow{g} D \quad D \xrightarrow{h} B}{C \xrightarrow{g\cdot h} B}\,\mathtt{C}}{A \xrightarrow{f\cdot(g\cdot h)} B}\,\mathtt{C}\,,$$

Éléments neutres.

$$\frac{\dfrac{}{A \xrightarrow{\mathrm{id}_A} A}\,\mathtt{I} \qquad A \xrightarrow{f} B}{A \xrightarrow{\mathrm{id}_A\cdot f} B}\,\mathtt{C} \quad = \quad A \xrightarrow{f} B \quad = \quad \frac{A \xrightarrow{f} B \qquad \dfrac{}{B \xrightarrow{\mathrm{id}_B} B}\,\mathtt{I}}{A \xrightarrow{f\cdot \mathrm{id}_B} B}\,\mathtt{C}\,.$$

En fait, dans (Lambek et Scott, 1988), cette famille d'exemples constitue *la définition* des catégories. Notons que la propriété des éléments neutres est une règle d'*élimination des coupures* : elle permet de diminuer le nombre d'occurrences de la règle de coupure dans certaines preuves. On dit qu'un système déductif a la *propriété d'élimination des coupures* si chaque preuve est égale à une preuve qui n'utilise pas la règle de coupure.

Les propriétés de la catégorie $\mathcal{S}$ sont alors encodées par les règles du système déductif **S**. Par exemple, l'existence d'un objet initial et d'un objet final correspondent, par la propriété universelle de ces objets, à l'existence des règles suivantes :

$$\frac{}{\mathbf{0} \xrightarrow{?_A} A}\,\mathtt{LAx} \qquad , \qquad \frac{}{A \xrightarrow{!_A} \mathbf{1}}\,\mathtt{RAx}\,.$$

On peut donc interpréter **0** et **1** respectivement comme l'*antilogie* et la *tautologie*.

La propriété universelle du produit (binaire), quant à elle, donne lieu aux trois règles suivantes :

$$\frac{Z \xrightarrow{f} A \quad Z \xrightarrow{g} B}{Z \xrightarrow{\langle f,g\rangle} A \times B}\,\mathtt{R}\times \quad , \quad \frac{}{A \times B \xrightarrow{\mathtt{pr}_0} A}\,\mathtt{Pr}_0 \quad , \quad \frac{}{A \times B \xrightarrow{\mathtt{pr}_1} B}\,\mathtt{Pr}_1 \,.$$

La forme de la règle $\mathtt{R}\times$ est la même que celle de la *conjonction à droite* du système **LK** de Gentzen. On peut également retrouver les règles de *conjonction à gauche* via une coupure comme ci-dessous, nous laissant interpréter le produit comme *étant* la conjonction.

$$\frac{A \xrightarrow{f} C}{A \times B \xrightarrow{f'} C}\,\mathtt{L}\times_0 \;:=\; \frac{\dfrac{}{A \times B \xrightarrow{\mathtt{pr}_0} A}\,\mathtt{Pr}_0 \qquad A \xrightarrow{f} C}{A \times B \xrightarrow{\mathtt{pr}_0 \cdot f} C}\,\mathtt{C}\,,$$

$$\frac{B \xrightarrow{f} C}{A \times B \xrightarrow{f'} C}\,\mathtt{L}\times_1 \;:=\; \frac{\dfrac{}{A \times B \xrightarrow{\mathtt{pr}_1} B}\,\mathtt{Pr}_1 \qquad B \xrightarrow{f} C}{A \times B \xrightarrow{\mathtt{pr}_1 \cdot f} C}\,\mathtt{C}\,.$$

Par dualité, si $\mathcal{S}$ admet les coproduits binaires, on peut interpréter ceux-ci comme étant la *disjonction* de formules et retrouver les règles suivantes :

$$\frac{A \xrightarrow{f} Z \quad B \xrightarrow{g} Z}{A + B \xrightarrow{\{f,g\}} Z}\,\mathtt{L}+ \quad , \quad \frac{C \xrightarrow{f} A}{C \xrightarrow{f \cdot \mathtt{in}_0} A + B}\,\mathtt{R}+_0 \quad , \quad \frac{C \xrightarrow{f} B}{C \xrightarrow{f \cdot \mathtt{in}_1} A + B}\,\mathtt{R}+_1 \,.$$

3.2 Règles des preuves circulaires

Soit $\mathcal{S} = \{X =_p F_X\}_{X \in \mathsf{BV}(S)}$ un système dirigé d'équations. On définit le système déductif $\mathbf{C}_\mathcal{S}$, dont l'ensemble des formules est l'ensemble $\mathfrak{F}$ de la section 2.4 et dont les règles d'inférence se trouvent dans le Tableau 3.1. Les preuves de ce système seront appelées ***pré-preuves circulaires sur*** $\mathcal{S}$ (on se garde de les appeler *preuves circulaires* pour l'instant pour des raisons qui seront détaillées à la Section 3.4). Remarquons que les règles de la colonne du Tableau 3.1 identifiée par $\mathfrak{L}$ agissent seulement sur le côté gauche des séquents, tandis que celles de la

colonne $\mathfrak{R}$ n'agissent que du côté droit. On peut donc partitionner l'ensemble Σ des (noms de) règles comme $\Sigma := \mathfrak{L} \cup \mathfrak{R} \cup \{\mathtt{I}, \mathtt{C}, \mathtt{H}\}$.

Identité, Coupure, Hypothèse	$\dfrac{}{A \vdash A}\,\mathtt{I}$ $\qquad$ $\dfrac{A \vdash C \quad C \vdash B}{A \vdash B}\,\mathtt{C}$ $\qquad$ $\dfrac{}{A \vdash B}\,\mathtt{H}$	
	$\mathfrak{L}$	$\mathfrak{R}$
Axiomes	$\dfrac{}{0 \vdash A}\,\mathtt{LAx}$	$\dfrac{}{A \vdash 1}\,\mathtt{RAx}$
Produit ($j \in \{0,1\}$)	$\dfrac{A_j \vdash B}{A_0 \times A_1 \vdash B}\,\mathtt{L}\times_j$	$\dfrac{A \vdash B_0 \quad A \vdash B_1}{A \vdash B_0 \times B_1}\,\mathtt{R}\times$
Coproduit ($j \in \{0,1\}$)	$\dfrac{A_0 \vdash B \quad A_1 \vdash B}{A_0 + A_1 \vdash B}\,\mathtt{L}+$	$\dfrac{A \vdash B_j}{A \vdash B_0 + B_1}\,\mathtt{R}+_j$
Points fixes ($\forall X \in \mathsf{BV}(\mathcal{S})$)	$\dfrac{F_X \vdash B}{X \vdash B}\,\mathtt{LF}_X$	$\dfrac{A \vdash F_X}{A \vdash X}\,\mathtt{RF}_X$

Tableau 3.1 Règles d'inférence du système $\mathbf{C}_{\mathcal{S}}$

Pour $V \subseteq \mathbb{V}$ suffisamment grand, chaque séquent $A \vdash B$ s'interprète comme une flèche $f : [\![A]\!]_V^{\mathcal{S}} \to [\![B]\!]_V^{\mathcal{S}}$ dans la catégorie $\mathcal{C}_V := \mathcal{F}un(\mathcal{C}^V, \mathcal{C})$, c'est-à-dire une transformation naturelle du foncteur $[\![A]\!] = [\![A]\!]_V^{\mathcal{S}}$ vers le foncteur $[\![B]\!] = [\![B]\!]_V^{\mathcal{S}}$. Les règles établissent alors des équations entre ces flèches. Notons que la plupart de ces équations sont déjà expliquées au Chapitre 2. Trois nouvelles règles font toutefois leur entrée : les deux règles de point fixe et la règle d'hypothèse.

Commençons par interpréter les règles de point fixe. D'un point de vue syntaxique, sachant que $X = F_X$, on se permet de substituer F_X par X dans les preuves. Sémantiquement parlant, la règle $\mathtt{LF}_X$ dit plutôt : « Étant donné une

flèche $f : [\![F_X]\!] \to [\![B]\!]$, on peut construire une flèche (canonique) $f' : [\![X]\!] \to [\![B]\!]$. » Alors déjà, pour s'assurer que $[\![X]\!]$ et $[\![F_X]\!]$ aient un sens, on exige que la catégorie dans laquelle on interprète la règle soit μ-bicomplète. Le lien canonique entre f et f' dépend alors de la nature du point fixe qu'est $[\![X]\!]$. Si $([\![X]\!], x)$ est l'algèbre initiale du foncteur $[\![F_X]\!]$, il suffit alors de poser $f' = \alpha_X^{-1} \cdot f$, où α_X est la flèche canonique donnée par la Proposition 2.9. Si $([\![X]\!], x)$ est plutôt la coalgèbre finale de $[\![F_X]\!]$, on pose plutôt $f' = \zeta_X \cdot f$, où, encore une fois, ζ_X est donnée par la Proposition 2.9. Un raisonnement analogue (dual) conduit à l'interprétation de la règle $\mathtt{RF}_X$.

Toutes ces interprétations sont résumées dans le Tableau 3.2. Une expression de la forme

$$\frac{\{F_i \xrightarrow{f_i} G_i\}_{i \in I}}{F \xrightarrow{g} G}\,\rho$$

dans ce tableau signifie qu'on souhaite définir une fonction

$$[\![\rho]\!] : \prod_{i \in I} \mathcal{C}_V(F_i, G_i) \to \mathcal{C}_V(F, G)$$

par l'équation $[\![\rho]\!](\vec{f}) = g$, où $\vec{f} = (f_i)_{i \in I}$ et chaque $f_i : F_i \to G_i$ est une transformation naturelle.

Enfin, quant à la règle d'hypothèse (manquante dans le Tableau 3.2), elle peut sembler surpuissante car elle permet de prouver n'importe quel séquent directement, mais il faut plutôt la voir comme un outil technique nous permettant de décomposer les preuves en morceaux. Les sommets marqués de la règle $\mathtt{H}$ constituent des sortes de variables qu'on se permettra de substituer par n'importe quelle flèche déjà définie (pourvu qu'elle ait le bon domaine et le bon codomaine). L'interprétation des preuves circulaires dépendra donc de ces variables.

Identité, Coupure	$\dfrac{}{[\![A]\!] \xrightarrow{\mathtt{id}_{[\![A]\!]}} [\![A]\!]}\,\mathtt{I}$	$\dfrac{[\![A]\!] \xrightarrow{f} [\![C]\!] \quad [\![C]\!] \xrightarrow{g} [\![B]\!]}{[\![A]\!] \xrightarrow{f \cdot g} [\![B]\!]}\,\mathtt{C}$
	$\mathfrak{L}$	$\mathfrak{R}$
Axiomes	$\dfrac{}{\mathbf{0} \xrightarrow{?_{[\![A]\!]}} [\![A]\!]}\,\mathtt{LAx}$	$\dfrac{}{[\![A]\!] \xrightarrow{!_{[\![A]\!]}} \mathbf{1}}\,\mathtt{RAx}$
Produit	$\dfrac{[\![A_j]\!] \xrightarrow{f} [\![B]\!]}{[\![A_0]\!] \times [\![A_1]\!] \xrightarrow{\mathtt{pr}_j \cdot f} [\![B]\!]}\,\mathtt{L}\times_j$	$\dfrac{[\![A]\!] \xrightarrow{f_0} [\![B_0]\!] \quad [\![A]\!] \xrightarrow{f_1} [\![B_1]\!]}{[\![A]\!] \xrightarrow{\langle f_0, f_1 \rangle} [\![B_0]\!] \times [\![B_1]\!]}\,\mathtt{R}\times$
Coproduit	$\dfrac{[\![A_0]\!] \xrightarrow{f_0} [\![B]\!] \quad [\![A_1]\!] \xrightarrow{f_1} [\![B]\!]}{[\![A_0]\!] + [\![A_1]\!] \xrightarrow{\{f_0, f_1\}} [\![B]\!]}\,\mathtt{L}+$	$\dfrac{[\![A]\!] \xrightarrow{f} [\![B_j]\!]}{[\![A]\!] \xrightarrow{f \cdot \mathtt{in}_j} [\![B_0]\!] + [\![B_1]\!]}\,\mathtt{R}+_j$
Points fixes (μ)	$\dfrac{[\![F_X]\!] \xrightarrow{f} [\![B]\!]}{[\![X]\!] \xrightarrow{\alpha_X^{-1} \cdot f} [\![B]\!]}\,\mathtt{LF}_X$	$\dfrac{[\![A]\!] \xrightarrow{f} [\![F_X]\!]}{[\![A]\!] \xrightarrow{f \cdot \alpha_X} [\![X]\!]}\,\mathtt{RF}_X$
Points fixes (ν)	$\dfrac{[\![F_X]\!] \xrightarrow{f} [\![B]\!]}{[\![X]\!] \xrightarrow{\zeta_X \cdot f} [\![B]\!]}\,\mathtt{LF}_X$	$\dfrac{[\![A]\!] \xrightarrow{f} [\![F_X]\!]}{[\![A]\!] \xrightarrow{f \cdot \zeta_X^{-1}} [\![X]\!]}\,\mathtt{RF}_X$

Tableau 3.2 Interprétation fonctionnelle des règles d'inférence de $\mathbf{C}_{\mathcal{S}}$

3.3 Exemples

Avant de faire les détails sur l'interprétation des preuves circulaires en général, il importe de faire quelques exemples qui illustrent de quelle façon on peut les utiliser. Tous ces exemples vivent dans la catégorie des ensembles et les pré-preuves circulaires peuvent donc être vues comme des programmes qui dénotent des fonctions.

Exemple 1. Souvenons-nous du chapitre précédent que l'ensemble des nombres naturels est le support $\mathbb{N}$ de l'algèbre initiale du foncteur $F(X) = \mathbf{1} + X$, avec la

structure $\mathbf{1} + \mathbb{N} \xrightarrow{\{0,\mathtt{suc}\}} \mathbb{N}$. Pour décrire des fonctions numériques $f : \mathbb{N} \to \mathbb{N}$ à l'aide des pré-preuves circulaires, il faut donc au moins se donner le système à une seule équation $\mathcal{S} = \{N =_1 1 + N\}$, de façon à avoir $[\![N]\!] = \mathbb{N}$.

Soit `double` : $\mathbb{N} \to \mathbb{N}$ la fonction qui envoie n sur $2n$. On peut la définir récursivement comme suit :

$$\begin{aligned} \mathtt{double}(0) &= 0 \\ \mathtt{double}(\mathtt{Suc}\ n) &= \mathtt{Suc}(\mathtt{Suc}(\mathtt{double}(n))) \ . \end{aligned}$$

De cette définition récursive, on peut extraire la pré-preuve circulaire qui se trouve à la Figure 3.1. Pour ce premier exemple, on explicite les détails de cette correspondance.

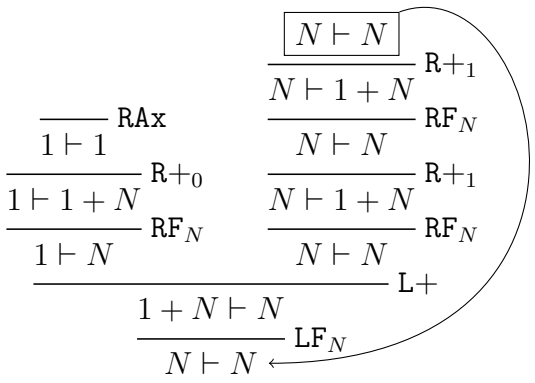


Figure 3.1 Une preuve circulaire représentant la fonction `double` : $\mathbb{N} \to \mathbb{N}$

Il faut lire la preuve à partir de la racine, c'est-à-dire de bas en haut. L'entrée du programme est stockée à gauche du symbole $\vdash$ tandis que sa sortie est stockée à droite. D'abord, la règle $\mathtt{LF}_N$ est utilisée pour obtenir la définition de N, pour savoir quelles sont les entrées possibles : il peut s'agir de 0 ou bien d'un successeur. On utilise ensuite L+ pour faire le branchement entre ces deux possibilités. Il faut

noter que la valeur stockée à gauche de $\vdash$ dans le sommet en-haut à droite de la règle $\mathtt{L}+$ n'est plus la même que ce qu'elle était à la racine (c'est maintenant son prédécesseur). Ainsi, les opérations de lecture sont destructives. Les règles droites, en contrepartie, représentent les choix de constructeurs qui constituent la sortie. Ainsi, dans le cas où l'entrée est 0, on utilise la règle $\mathtt{RF}_N$ pour savoir quels sont les constructeurs à notre portée (0 ou bien `Suc`) puis on choisit 0 grâce à la règle $\mathtt{R}+_0$. Sinon, c'est-à-dire dans le cas où l'entrée était un successeur, on applique deux fois `Suc` (avec la règle $\mathtt{RF}_X$ suivie de $\mathtt{R}+_1$) et, ensuite, il faut appliquer la fonction `double`. Or il se trouve que `double` est précisément la fonction qu'on tente de construire depuis la racine. Donc on boucle pour répéter le processus (d'où la circularité). ■

Simplement pour clarifier la notation avec la flèche : le sommet encadré et celui vers lequel il pointe sont en fait *le même sommet du graphe sous-jacent*. La flèche n'est donc pas une règle d'inférence.

Exemple 2. Afin d'illustrer l'utilité de la règle d'hypothèse `H`, supposons qu'on dispose d'une fonction $f : [\![A]\!] \to [\![B]\!]$ et qu'on veuille représenter, par une pré-preuve circulaire, la fonction $\mathtt{map}_f : [\![A]\!]^* \to [\![B]\!]^*$ qui associe, à une liste d'éléments de $[\![A]\!]$, la liste des images de ces éléments (voir l'Exemple 5 de la Section 2.2). On peut définir $\mathtt{map}_f$ récursivement comme suit :

$$\mathtt{map}_f(\varepsilon) = \mathtt{Nil}\,,$$
$$\mathtt{map}_f(a{:}w) = f(a){:}\mathtt{map}_f(w)\,.$$

Rappelons que, pour $X \in \{A, B\}$, $[\![X]\!]^* = [\![X^*]\!]$ où X^* est la variable de l'équation $X^* =_\mu 1 + (X \times X^*)$. En suivant un raisonnement analogue à l'exemple précédent, on peut donc représenter $\mathtt{map}_f$ par la pré-preuve circulaire de la Figure 3.2.

Il faut noter que la fonction f n'apparaît pas explicitement dans cette pré-preuve. C'est qu'il s'agit d'une pré-preuve avec une variable (une hypothèse), qu'on pour-

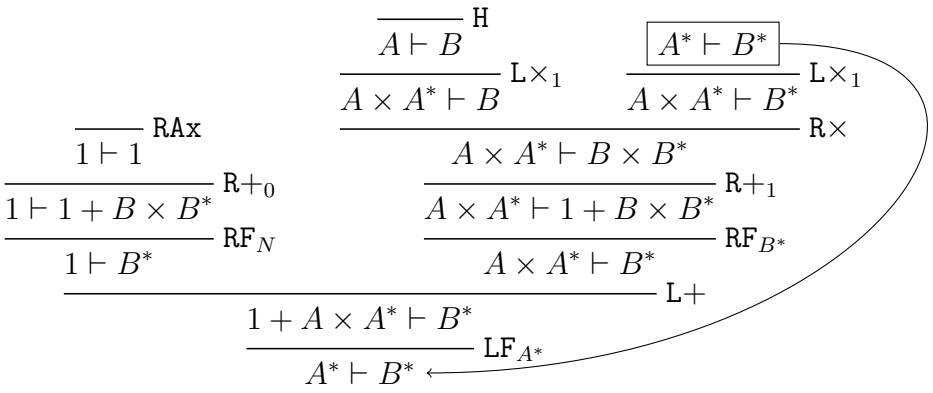


Figure 3.2 Une preuve circulaire représentant la fonction $\mathtt{map}_f$

rait substituer par f dans l'interprétation. Si f est elle-même représentée par une pré-preuve, l'effet est simplement d'aller coller la pré-preuve qui représente f à l'endroit où se trouve l'hypothèse. ■

Dans le reste de cette thèse, lorsqu'on voudra spécifier explicitement quelle est la flèche f ou la pré-preuve Π qu'on substituera à une hypothèse, on se permettra d'écrire la chose suivante :

$$\frac{\quad}{A \vdash B}\, f \quad \text{ou} \quad \frac{\quad}{A \vdash B}\, \Pi \quad \text{au lieu de} \quad \frac{\quad}{A \vdash B}\, \mathtt{H}.$$

Remarquons toutefois que la pré-preuve Π pourrait elle-même contenir des hypothèses. En ordonnant celles-ci de 0 à n et en supposant que le séquent de la i-ème hypothèse soit $A_i \vdash B_i$, cela permet d'utiliser les pré-preuves comme de nouvelles règles d'inférence en écrivant ceci :

$$\frac{A_0 \vdash B_0 \quad A_1 \vdash B_1 \quad \ldots \quad A_n \vdash B_n}{A \vdash B}\, \Pi \quad \text{ou encore} \quad \frac{\{A_i \vdash B_i\}_{i=0}^{n}}{A \vdash B}\, \Pi.$$

Exemple 3. Passons à un exemple coinductif. Rappelons que l'ensemble des suites infinies sur un alphabet (dans ce cas-ci, l'alphabet $[\![2]\!]$ a deux éléments) est la

solution pour S du système suivant :

$$\left\{ \begin{array}{l} S =_\nu 2 \times S \\ 2 =_\nu 1 + 1 \end{array} \right\}.$$

Supposons qu'on veuille définir la suite alternée $\texttt{alt} = (0, 1, 0, 1, 0, 1, \ldots)$ par une pré-preuve circulaire. Ceci est un élément de $[\![S]\!]$ et non pas une fonction à proprement parler, mais il y a correspondance évidente entre les suites $s \in [\![S]\!]$ et les fonctions de la forme $s : \mathbf{1} \to [\![S]\!]$. On optera donc pour une pré-preuve du séquent $1 \vdash S$. On peut définir `alt` corécursivement par l'équation suivante :

$$\texttt{alt} = \texttt{Cons}(0, \texttt{Cons}(1, \texttt{alt})).$$

Ce qui conduit à la pré-preuve circulaire de la Figure 3.3.

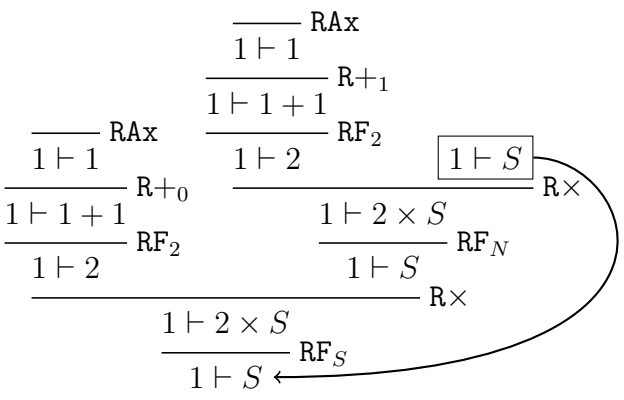


Figure 3.3 Une preuve circulaire représentant la suite alternée

■

Exemple 4. Faisons l'exercice à l'envers. Avec les mêmes équations que dans l'exemple précédent, considérons la pré-preuve circulaire de la Figure 3.4.

Quelle est la fonction $s : \mathbf{1} \to [\![S]\!]$ dénotée par la racine de cette pré-preuve ? En utilisant le Tableau 3.2 (ou en lisant la pré-preuve étape par étape comme dans l'Exemple 1), on trouve que celle-ci doit satisfaire l'équation implicite suivante :

$$s = \texttt{Cons}(0, \texttt{tail}(s)).$$

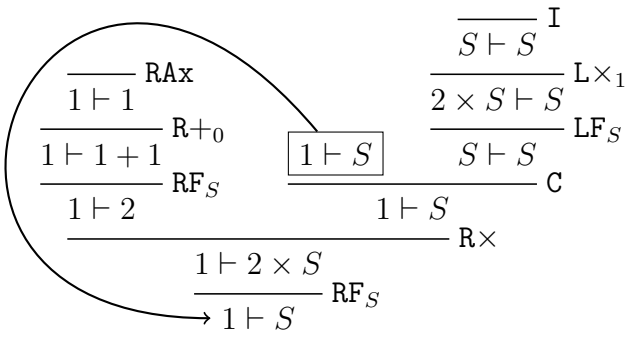


Figure 3.4 Une mystérieuse pré-preuve circulaire...

Or, plusieurs suites satisfaisant cette équation existent, à savoir, toutes les suites commençant par 0 ! Cette pré-preuve ne dénote donc pas une solution unique. Lorsqu'implémentée en Haskell, le programme entre simplement dans une boucle infinie puisqu'il n'arrive jamais à déterminer le second terme de la suite. ■

3.4 Conditions de garde

On veut exclure de notre syntaxe les preuves dont l'interprétation n'est pas bien définie, comme celle de l'Exemple 4 de la section précédente. Les pré-preuves survivant à cette exclusion seront celles qu'on appellera des *preuves*.

Dans les composantes sans cycles d'une pré-preuve circulaire, le problème ne se pose pas : on peut calculer l'unique expression de la racine récursivement à partir des feuilles en utilisant le Tableau 3.2. Ce sont donc les cycles qui sont problématiques. Or, dans le système sans coupures de Santocanale (2001), une condition de garde est formulée à propos des cycles. Il suffit de la généraliser. Celle-ci est inspirée de la théorie des jeux de parité (Section 2.5). Selon l'interprétation des pré-preuves par des programmes, la condition de garde dit intuitivement ceci :

Condition de garde (Intuitive)**.** *À chaque tour d'un cycle, ou bien le programme*

déconstruit un morceau de son entrée inductive (il se ramène vers les cas de base), ou bien il construit un morceau de sa sortie coinductive (il repousse le problème vers l'infini).

Formellement, soit Π une pré-preuve circulaire sur $\mathcal{S}$ et $\Gamma \subseteq \Pi$ un chemin, ou encore un sous-ensemble de sommets. Considérons les deux ensembles suivants.

$$L(\Gamma) := \{p_X : X \in \mathsf{BV}(\mathcal{S}) \text{ et } \exists u \in \Gamma \text{ t.q. } \textsc{Règ}(u) = \mathtt{LF}_X\},$$
$$R(\Gamma) := \{p_X : X \in \mathsf{BV}(\mathcal{S}) \text{ et } \exists u \in \Gamma \text{ t.q. } \textsc{Règ}(u) = \mathtt{RF}_X\}.$$

On dit que Γ a ***la propriété μ*** si $L(\Gamma) \neq \varnothing$ et $\max(L(\Gamma))$ est un nombre impair. En d'autres mots, la propriété μ dit que la structure lue avec la plus grande priorité dans Γ est inductive. Symétriquement, on dira que Γ a ***la propriété ν*** si $R(\Gamma) \neq \varnothing$ et $\max(R(\Gamma))$ est un nombre pair.

La condition de garde telle qu'énoncée intuitivement plus haut serait alors la suivante : chaque cycle dans Π a la propriété μ ou la propriété ν. C'est, en effet, la condition qu'on trouve dans Santocanale (2001). Mais il faut faire attention à la règle de coupure. En effet, quatre sortes de coupures peuvent survenir dans une pré-preuve circulaire. Si $\textsc{Règ}(u) = \mathtt{C}$, on dit que u est une coupure *gauche* si $\varsigma_0 u \twoheadrightarrow u$, *droite* si $\varsigma_1 u \twoheadrightarrow u$, *acyclique* si elle n'est ni gauche ni droite, et *ambidextre* si elle est gauche et droite (voir Tableau 3.3).

Naturellement, un cycle ne peut contenir aucune coupure acyclique : ce ne sont donc pas celles-ci qui sont problématiques. Si on regarde les coupures gauches, plus précisément le lien entre $\textsc{Seq}(u) = A \vdash B$ et $\textsc{Seq}(\varsigma_0 u) = A \vdash C$, on remarque que la formule gauche (A) est préservée d'un sommet à l'autre, mais qu'il n'y a *a priori* aucun lien entre les formules droites (C et B). Si donc le programme, en parcourant le cycle Γ, était en train de construire quelque chose à droite, son historique se trouve à être effacé en poursuivant vers la gauche. La construction n'aboutit donc

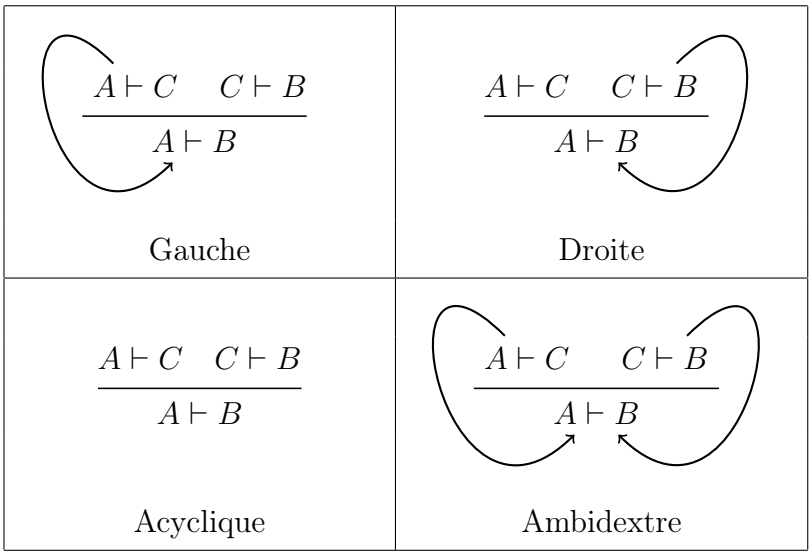


Tableau 3.3 Quatre sortes de coupures

pas en un tour de cycle, et c'est quelque chose qu'on doit éviter. Ainsi, on dira que Γ a une ***ν-trace droite*** si Γ a la propriété ν et s'il ne contient aucune coupure gauche (ni ambidextre). Symétriquement, Γ a une ***μ-trace gauche*** s'il a la propriété μ et s'il ne contient aucune coupure droite (ni ambidextre). On peut maintenant formuler la condition de garde.

Condition de garde G1 (Sur les cycles)**.** *Chaque cycle de* Π *a soit une* μ*-trace gauche ou une* ν*-trace droite.*

Une conséquence immédiate de cette condition est que les coupures ambidextres sont à proscrire complètement. D'autres systèmes basés sur des preuves circulaires, e.g. (Brotherston, 2005), formulent une condition dite de *traçabilité* en termes des chemins infinis plutôt que des cycles. Dans notre cas, cela donne la condition suivante, qu'on utilisera principalement au Chapitre 5.

Condition de garde G2 (Sur les chemins infinis)**.** *Chaque chemin infini* Γ *de* Π *peut être factorisé en* $\Gamma = \Gamma_0 \cdot \Gamma_1$ *où* Γ_0 *est fini,* Γ_1 *a soit une* μ*-trace gauche ou une* ν*-trace droite, et chaque règle de point fixe utilisée dans* Γ_1 *y est utilisée*

infiniment souvent.

Ces deux conditions ont le défaut de reposer sur une propriété devant être satisfaite par, en général, une infinité d'individus (*tous les cycles* ou *tous les chemins infinis*). Cela pose un problème algorithmique : comment vérifier, en temps fini, qu'une pré-preuve donnée satisfait l'une de ces conditions ? Heureusement, on peut encore reformuler la condition de garde en une propriété à vérifier sur *tous les sous-graphes fortement connexes* (Section 1.4), dont il n'y a qu'une quantité finie, rendant ainsi le problème décidable. C'est d'ailleurs sous une telle forme qu'est formulée la condition de *décharge d'induction de base*† dans (Sprenger et Dam, 2003), qui a inspiré celle de (Brotherston, 2005).

Condition de garde G3 (Sur les sous-graphes fortement connexes)**.** *Le support de chaque sous-graphe fortement connexe non trivial de* Π *a soit une* μ*-trace gauche ou une* ν*-trace droite.*

Proposition 3.1. *Si* Π *est une pré-preuve finie, alors les trois conditions de garde sont équivalentes.*

Démonstration.
G1 $\Rightarrow$ **G3 :** Soit $K \subseteq \Pi$ un sous-graphe fortement connexe contenant plus d'un sommet. Alors il existe un cycle Γ qui parcourt entièrement K. La condition **G1** appliquée à Γ entraîne alors facilement la condition **G3** sur K.

G3 $\Rightarrow$ **G2 :** Soit $\Gamma = (u, \gamma)$ un chemin infini dans Π. Puisque Π est finie, il existe un préfixe $\alpha \sqsubseteq \gamma$ tel que chaque sommet apparaissant un nombre fini de fois seulement dans Γ le fasse dans le segment initial $\Gamma_0 = (u, \alpha)$. Soit β tel que $\alpha \cdot \beta = \gamma$, $u' = \varsigma_\alpha u$ et $\Gamma_1 = (u', \beta)$, de sorte que l'on ait $\Gamma = \Gamma_0 \cdot \Gamma_1$.

---

†. Originalement : *basic induction discharge condition*

Pour $n \in \mathbb{N}$, soit $v_n = \Gamma_1(n)$ et soit K le graphe constitué des sommets et arêtes visitées par Γ_1. Notons d'abord que par construction, pour chaque $v \in K$, il existe une infinité de $n \in \mathbb{N}$ tels que $v_n = v$. Soit donc $v_m, v_n \in K$ avec $m < n$. Puisque Γ_1 est un chemin, alors $v_m \twoheadrightarrow_K v_n$. Mais puisque v_m apparaît infiniment souvent dans Γ_1, alors il existe $m' > n$ tel que $v_m = v_{m'}$. Ainsi, $v_n \twoheadrightarrow_K v_{m'} = v_m$. Il s'ensuit que K est fortement connexe. De plus, K contient plus d'un seul sommet parce que les règles du système $\mathbf{C}_\mathcal{S}$ ne permettent de construire aucune pré-preuve contenant une boucle de longueur 1. La condition **G3** appliquée à K implique alors que Γ_1 a une μ-trace gauche (si K a une μ-trace gauche) ou une ν-trace droite (si K a une ν-trace droite).

G2 $\Rightarrow$ G1 : Soit $\Gamma = (u, \gamma)$ un cycle dans Π. Alors $\Gamma^\omega := (u, \gamma\gamma\cdots)$ est un chemin infini dans Π. Puisque Γ^ω est périodique, il est facile de constater que la condition **G2** appliquée à Γ^ω entraîne la condition **G1** sur Γ. □

Définition. Une ***preuve circulaire*** est une pré-preuve finie Π satisfaisant les conditions de garde.

Remarquons enfin que les pré-preuves présentées dans les exemples 1 à 3 de la Section 3.3 sont des *vraies* preuves circulaires : elles satisfont les conditions de garde. Ce n'est pas le cas de l'exemple 4, ce qui peut expliquer que celle-ci ne dénote aucune fonction.

Il faut toutefois être prudent avec cette affirmation. On va effectivement montrer dans la prochaine section que les conditions de garde assurent l'adéquation du système de preuves. Au Chapitre 5, on rajoutera l'élimination des coupures aux propriétés que garantissent les conditions de garde. On verra toutefois au Chapitre 7 que les conditions de garde ne sont pas des conditions nécessaires pour avoir ces propriétés, mais seulement des conditions suffisantes.

Lemme 3.2. *Soit* Π *une preuve circulaire et soit* Γ *un chemin infini dans* Π. *Alors il existe* $n_0 \in \mathbb{N}$ *tel que* $\forall n \geq n_0$, *si* $\text{RÈG}(\Gamma(n)) = \mathtt{C}$, *alors :*

– $\Gamma(n+1) = \varsigma_0(\Gamma(n))$ *si* Γ *a une* μ*-trace gauche ;*

– $\Gamma(n+1) = \varsigma_1(\Gamma(n))$ *si* Γ *a une* ν*-trace droite.*

Démonstration. On démontre le cas où Γ a une μ-trace gauche, la démonstration de l'autre cas étant symétrique à celle-ci. Supposons, au contraire, qu'il existe une suite infinie d'indices :

$$n_1 < n_2 < n_3 < \ldots \in \mathbb{N}$$

tels que $\forall k$, $\Gamma(n_k + 1) = \varsigma_1(\Gamma(n_k))$. Puisque Π est un graphe fini, alors par le principe des nids de pigeons, on peut trouver un sommet $u \in \Pi$ et une autre suite

$$k_1 < k_2 < k_3 < \ldots \in \mathbb{N}$$

telle que $\forall j \in \mathbb{N}$, $\Gamma(n_{k_j}) = u$. Or, puisque Γ est un chemin, alors on a

$$\varsigma_1 u = \varsigma_1 \Gamma(n_{k_1}) = \Gamma(n_{k_1} + 1) \twoheadrightarrow \Gamma(n_{k_2}) = u \ .$$

Donc u est une coupure droite. Mais puisque Γ visite u infiniment souvent, on a une contradiction avec le fait que Γ ait une μ-trace gauche. □

CHAPITRE IV

SÉMANTIQUE DÉNOTATIONNELLE

Dans ce chapitre, on démontre l'adéquation et la plénitude des preuves circulaires en tant qu'outil syntaxique pour dénoter les flèches des catégories μ-bicomplètes libres. Plus précisément, comme on l'a vu dans les exemples du Chapitre 3, toute preuve circulaire Π peut être traduite en un système d'équations $[\![?\Pi]\!]$ via le Tableau 3.2. La propriété d'*adéquation* signifie que dans toute catégorie μ-bicomplète $\mathcal{C}$, ce système admet une solution unique. Réciproquement, la propriété de *plénitude* signifie que toute flèche d'une catégorie μ-bicomplète libre est la solution (en un sommet donné) du système d'équations associé à une certaine preuve circulaire. Les résultats de ce chapitre sont présentés dans (Fortier et Santocanale, 2013, 2014).

4.1 Naturalité des règles

On commence par donner une autre interprétation des règles de $\mathbf{C}_{\mathcal{S}}$, à l'exception des règles d'identité, de coupure et d'hypothèse, en tant que transformations naturelles entre hom-foncteurs généralisés. En effet, le Tableau 4.1 contient des expressions de la forme

$$\frac{\{F_i x_0 \xrightarrow{h_i} G_i x_1\}_{i\in I}}{Fx_0 \xrightarrow{g} Gx_1}\,\rho$$

qui signifient que pour toute paire d'objets $x_0, x_1 \in \mathcal{C}^V$ et des foncteurs $F_i, G_i, F, G : \mathcal{C}^V \to \mathcal{C}$, on définit une fonction

$$[\rho]_{x_0,x_1} : \prod_{i\in I} \mathcal{C}(F_i x_0, G_i x_1) \to \mathcal{C}(Fx_0, Gx_1)$$

par l'équation $[\rho]_{x_0,x_1}(\vec{h}) = g$, où $\vec{h} = (h_i)_{i\in I}$. Notons que chaque $h_i : F_i x_0 \to G_i x_1$ est une flèche de $\mathcal{C}$ et non pas de $\mathcal{C}_V = \mathcal{F}un(\mathcal{C}^V, \mathcal{C})$ comme dans le Tableau 3.2.

	$\mathfrak{L}$	$\mathfrak{R}$
Axiomes	$\dfrac{}{\mathbf{0} \xrightarrow{?_{Gx_1}} Gx_1}\ \mathtt{LAx}$	$\dfrac{}{Fx_0 \xrightarrow{!_{Fx_0}} \mathbf{1}}\ \mathtt{RAx}$
Produit	$\dfrac{F_j x_0 \xrightarrow{h} Gx_1}{F_0x_0 \times F_1x_0 \xrightarrow{\mathtt{pr}_{i;x_0}\cdot h} Gx_1}\ \mathtt{L}\times_j$	$\dfrac{Fx_0 \xrightarrow{h} G_0x_1 \quad Fx_0 \xrightarrow{k} G_1x_1}{Fx_0 \xrightarrow{\langle h,k\rangle} G_0x_1 \times G_1x_1}\ \mathtt{R}\times$
Coproduit	$\dfrac{F_0x_0 \xrightarrow{h} Gx_1 \quad F_1x_0 \xrightarrow{k} Gx_1}{F_0x_0 + F_1x_0 \xrightarrow{\{h,k\}} Gx_1}\ \mathtt{L}+$	$\dfrac{Fx_0 \xrightarrow{h} G_jx_1}{Fx_0 \xrightarrow{h\cdot \mathtt{in}_{j;x_1}} G_0x_1 + G_1x_1}\ \mathtt{R}+_j$
Points fixes (μ)	$\dfrac{[\![F_X]\!](x_0) \xrightarrow{h} Gx_1}{[\![X]\!](x_0) \xrightarrow{\alpha^{-1}_{X;x_0}\cdot h} Gx_1}\ \mathtt{LF}_X$	$\dfrac{Fx_0 \xrightarrow{h} [\![F_X]\!](x_1)}{Fx_0 \xrightarrow{h\cdot \alpha_{X;x_1}} [\![X]\!](x_1)}\ \mathtt{RF}_X$
Points fixes (ν)	$\dfrac{[\![F_X]\!](x_0) \xrightarrow{h} Gx_1}{[\![X]\!](x_0) \xrightarrow{\zeta_{X;x_0}\cdot h} Gx_1}\ \mathtt{LF}_X$	$\dfrac{Fx_0 \xrightarrow{h} [\![F_X]\!](x_1)}{Fx_0 \xrightarrow{h\cdot \zeta^{-1}_{X;x_1}} [\![X]\!](x_1)}\ \mathtt{RF}_X$

Tableau 4.1 Interprétation naturelle des règles d'inférence de $\mathbf{C}_\mathcal{S}$

Or, rappelons qu'étant donné deux foncteurs $F, G : \mathcal{C}^V \to \mathcal{C}$, on a défini le foncteur $\mathcal{C}(F, G)$ à la Section 2.1 par la composition suivante :

$$\overline{\mathcal{C}^V} \times \mathcal{C}^V \xrightarrow{\overline{F}\times G} \overline{\mathcal{C}} \times \mathcal{C} \xrightarrow{\mathcal{C}(\_,\_)} \mathcal{E}ns\,.$$

On dénotera, par la suite, les objets de $\overline{\mathcal{C}^V} \times \mathcal{C}^V$ par $x = (\overline{x_0}, x_1)$ ou $y = (\overline{y_0}, y_1)$ pour $x_0, x_1, y_0, y_1 \in \mathcal{C}^V$. Par abus de langage, on écrira aussi $[\rho]_x$ au lieu de $[\rho]_{x_0,x_1}$, où $x = (\overline{x_0}, x_1) \in \overline{\mathcal{C}^V} \times \mathcal{C}^V$. Soit $[\rho] = \big([\rho]_x\big)_{x\in\overline{\mathcal{C}^V}\times\mathcal{C}^V}$.

Proposition 4.1. *Si $\rho \notin \{\mathtt{I}, \mathtt{C}, \mathtt{H}\}$, alors $[\rho]$ est une transformation naturelle*

$$[\rho] : \prod_{i \in I} \mathcal{C}(F_i, G_i) \to \mathcal{C}(F, G).$$

Démonstration. Vérifions pour chaque $\rho \notin \{\mathtt{I}, \mathtt{C}\}$.

– $\underline{\mathtt{LAx} \text{ et } \mathtt{RAx}}$: Comme ces règles n'ont aucune hypothèse, le domaine de $[\rho]$ est le singleton $\mathbf{1}$. De plus, si $\rho = \mathtt{LAx}$, alors $F \equiv \mathbf{0}$ et si $\rho = \mathtt{RAx}$, alors $G \equiv \mathbf{1}$. Dans les deux cas, la propriété universelle implique que pour tout $y \in \overline{\mathcal{C}^V} \times \mathcal{C}^V$, $\mathcal{C}(Fy_0, Gy_1)$ est un singleton. Puisque $\mathbf{1}$ est l'objet terminal de $\mathcal{E}\mathit{ns}$, il existe une unique flèche $\mathbf{1} \to \mathbf{1}$. En particulier, pour toute flèche $f : x \to y$ de $\overline{\mathcal{C}^V} \times \mathcal{C}^V$, $[\rho]_y = [\rho]_x \cdot \mathcal{C}(F, G)(f)$, ce qui établit la naturalité de $[\rho]$.

– $\underline{\mathtt{L}\times_i \text{ et } \mathtt{LF}_X}$: Ici, $[\rho]_x$ est de la forme

$$\begin{aligned} [\rho]_x : \mathcal{C}(F_0 x_0, G x_1) &\to \mathcal{C}(F x_0, G x_1) \,, \\ h &\mapsto \beta_{x_0} \cdot h \,, \end{aligned}$$

où $\beta : F \to F_0$ est une transformation naturelle ($\beta \in \{\mathtt{pr}_i, \alpha_X^{-1}, \zeta_X\}$). Pour toute flèche $f : x \to y$ de $\overline{\mathcal{C}^V} \times \mathcal{C}$ et tout $h \in \mathcal{C}(F_0 x_0, G x_1)$, on a alors :

$$\begin{aligned} \big([\rho]_y \circ \mathcal{C}(F_0, G)(f)\big)(h) &= [\rho]_y (F_0 u \cdot h \cdot G v) \\ &= \beta_{y_0} \cdot F_0 u \cdot h \cdot G v \\ &= F u \cdot \beta_{x_0} \cdot h \cdot G v \qquad \text{(par naturalité de } \beta) \\ &= \mathcal{C}(F, G)(f)(\beta_{x_0} \cdot h) \\ &= \big(\mathcal{C}(F, G)(f) \circ [\rho]_x\big)(h) \,. \end{aligned}$$

Ainsi, $[\rho]_y \circ \mathcal{C}(F_0, G)(f) = \mathcal{C}(F, G)(f) \circ [\rho]_x$, ce qui établit la naturalité de $[\rho]$.

– $\underline{\mathtt{R}+_i \text{ et } \mathtt{RF}_X}$: Similairement au cas précédent, $[\rho]_x$ est de la forme

$$\begin{aligned} [\rho]_x : \mathcal{C}(F x_0, G_0 x_1) &\to \mathcal{C}(F x_0, G x_1) \,, \\ h &\mapsto h \cdot \beta_{x_1} \,, \end{aligned}$$

où $\beta : G_0 \to G$ est une transformation naturelle ($\beta \in \{\mathtt{in}_i, \alpha_X, \zeta_X^{-1}\}$). Pour toute flèche $f : x \to y$ de $\overline{\mathcal{C}^V} \times \mathcal{C}$ et tout $h \in \mathcal{C}(Fx_0, G_0x_1)$, on a alors :

$$\begin{aligned}
\big([\rho]_y \circ \mathcal{C}(F, G_0)(f)\big)(h) &= [\rho]_y(Fu \cdot h \cdot G_0 v) \\
&= Fu \cdot h \cdot G_0 v \cdot \beta_{y_1} \\
&= Fu \cdot h \cdot \beta_{x_1} \cdot Gv \qquad \text{(par naturalité de } \beta) \\
&= \mathcal{C}(F, G)(f)(h \cdot \beta_{x_1}) \\
&= \big(\mathcal{C}(F, G)(f) \circ [\rho]_x\big)(h)\,.
\end{aligned}$$

Ainsi, $[\rho]_y \circ \mathcal{C}(F_0, G)(f) = \mathcal{C}(F, G)(f) \circ [\rho]_x$, ce qui établit la naturalité de $[\rho]$.

– $\underline{\mathtt{R}\times}$: Ici, $[\rho]_x$ est de la forme

$$\begin{aligned}
[\rho]_x : \mathcal{C}(Fx_0, G_0x_1) \times \mathcal{C}(Fx_0, G_1x_1) &\to \mathcal{C}(Fx_0, Gx_1)\,, \\
(h, k) &\mapsto \langle h, k\rangle\,,
\end{aligned}$$

où $G = G_0 \times G_1 : \mathcal{C}^V \to \mathcal{C}$ est le foncteur donné par l'équation

$$G(\xi) = G_0(\xi) \times G_1(\xi)$$

où ξ est un objet ou une flèche de $\mathcal{C}^V$. Pour toute flèche $f : x \to y$ de $\overline{\mathcal{C}^V} \times \mathcal{C}$ et toute paire $(h, k) \in \mathcal{C}(Fx_0, G_0x_1) \times \mathcal{C}(Fx_0 \times G_1x_1)$, on a alors :

$$\begin{aligned}
&\big([\rho]_y \circ (\mathcal{C}(F, G_0) \times \mathcal{C}(F, G_1))(f)\big)(h, k) \\
&\qquad = \big([\rho]_y \circ (\mathcal{C}(F, G_0)(f) \times \mathcal{C}(F, G_1)(f))\big)(h, k) \\
&\qquad = [\rho]_y\big(\mathcal{C}(F, G_0)(f)(h), \mathcal{C}(F, G_1)(f))(k)\big) \\
&\qquad = [\rho]_y\big(Fu \cdot h \cdot G_0 v\ ,\ Fu \cdot k \cdot G_1 v\big) \\
&\qquad = \langle Fu \cdot h \cdot G_0 v\ ,\ Fu \cdot k \cdot G_1 v\rangle \\
&\qquad = \langle Fu \cdot h\ ,\ Fu \cdot k\rangle \cdot (G_0 v \times G_1 v) \\
&\qquad = \big(Fu \cdot \langle h, k\rangle\big) \cdot (G_0 \times G_1)(v) \\
&\qquad = Fu \cdot \langle h, k\rangle \cdot Gv
\end{aligned}$$

$$
\begin{aligned}
&= \mathcal{C}(F,G)(f)(\langle h,k\rangle) \\
&= \big(\mathcal{C}(F,G)(f)\circ[\rho]_x\big)(h,k)\,.
\end{aligned}
$$

Ainsi, $[\rho]_y \circ (\mathcal{C}(F,G_0)\times\mathcal{C}(F,G_1))(f) = \mathcal{C}(F,G)(f)\circ[\rho]_x$, ce qui établit la naturalité de $[\rho]$.

– $\underline{\mathtt{L}+}$: Similairement au cas précédent, $[\rho]_x$ est de la forme

$$
\begin{aligned}
[\rho]_x : \mathcal{C}(F_0x_0, Gx_1)\times\mathcal{C}(F_1x_0,Gx_1) &\to \mathcal{C}(Fx_0,Gx_1)\,, \\
(h,k) &\mapsto \{h,k\}\ ,
\end{aligned}
$$

où $F = F_0 + F_1 : \mathcal{C}^V \to \mathcal{C}$ est le foncteur donné par l'équation

$$F(\xi) = F_0(\xi) + F_1(\xi)$$

où ξ est un objet ou une flèche de $\mathcal{C}^V$. Pour toute flèche $f : x \to y$ de $\overline{\mathcal{C}^V}\times\mathcal{C}$ et toute paire $(h,k)\in\mathcal{C}(F_0x_0,Gx_1)\times\mathcal{C}(F_1x_0\times Gx_1)$, on a alors :

$$
\begin{aligned}
&\big([\rho]_y\circ(\mathcal{C}(F_0,G)\times\mathcal{C}(F_1,G))(f)\big)(h,k) \\
&\qquad = \big([\rho]_y\circ(\mathcal{C}(F_0,G)(f)\times\mathcal{C}(F_1,G)(f))\big)(h,k) \\
&\qquad = [\rho]_y\big(\mathcal{C}(F_0,G)(f)(h),\mathcal{C}(F_1,G)(f))(k)\big) \\
&\qquad = [\rho]_y\big(F_0u\cdot h\cdot Gv\ ,\ F_1u\cdot k\cdot Gv\big) \\
&\qquad = \{F_0u\cdot h\cdot Gv\ ,\ F_1u\cdot k\cdot Gv\} \\
&\qquad = (F_0u+F_1u)\cdot\{h\cdot Gv\ ,\ k\cdot Gv\} \\
&\qquad = (F_0+F_1)(u)\cdot\big(\{h,k\}\cdot Gv\big) \\
&\qquad = Fu\cdot\{h,k\}\cdot Gv \\
&\qquad = \mathcal{C}(F,G)(f)(\{h,k\}) \\
&\qquad = \big(\mathcal{C}(F,G)(f)\circ[\rho]_x\big)(h,k)\,.
\end{aligned}
$$

Ainsi, $[\rho]_y\circ(\mathcal{C}(F_0,G)\times\mathcal{C}(F_1,G))(f) = \mathcal{C}(F,G)(f)\circ[\rho]_x$, ce qui établit la naturalité de $[\rho]$. □

On peut retrouver la fonction $[\![\rho]\!] : \prod_{i\in I} \mathcal{C}_V(F_i, G_i) \to \mathcal{C}_V(F, G)$ à partir de la transformation naturelle $[\rho]$ via la relation suivante. Soit $\vec{\beta} = (\beta^i)_{i\in I}$ un vecteur de transformations naturelles $\beta^i \in \mathcal{C}_V(F_i, G_i)$. Alors $[\![\rho]\!](\vec{\beta}) = \gamma$, où $\gamma = (\gamma_c)_{c\in\mathcal{C}}$ est définie par $\gamma_c := [\rho]_{c,c}(\vec{\beta_c})$. Il faut bien sûr vérifier que γ est naturelle avant d'affirmer que le codomaine de $[\![\rho]\!]$ est $\mathcal{C}_V(F, G)$. Cela est faisable directement à partir du Tableau 3.2, mais c'est aussi une conséquence du Lemme plus général suivant, qui sera aussi utile plus tard pour interpréter des morceaux de preuves comme des règles d'inférence généralisées.

Lemme 4.2. *Soit* $\alpha = (\alpha_{x_0,x_1})_{x\in\overline{\mathcal{C}^V}\times\mathcal{C}^V} : \prod_{i=1}^n \mathcal{C}(F_i, G_i) \to \mathcal{C}(F, G)$ *une transformation naturelle et, pour* $i = 1 \dots n$*, soit* $\beta^i \in \mathcal{C}_V(F_i, G_i)$*. Alors la collection* $\gamma = (\gamma_c)_{c\in\mathcal{C}^V}$ *de flèches de* $\mathcal{C}$ *définie par l'équation*

$$\gamma_c = \alpha_{c,c}(\beta^1_c, \dots, \beta^n_c) : Fc \to Gc$$

est une transformation naturelle de F *vers* G*.*

Démonstration. Soit $f : c \to d$ une flèche de $\mathcal{C}^V$. Alors :

$$\begin{aligned}
\gamma_c \cdot Gf &= \alpha_{c,c}(\beta^1_c, \dots \beta^n_c) \cdot Gf \\
&= \alpha_{c,d}(\beta^1_c \cdot G_1 f, \dots \beta^n_c \cdot G_n f) && \text{(naturalité de } \alpha_{x_0,x_1} \text{ en } x_1) \\
&= \alpha_{c,d}(F_1 f \cdot \beta^1_d, \dots F_n f \cdot \beta^n_d) && \text{(naturalité des } \beta^i) \\
&= Ff \cdot \alpha_{d,d}(\beta^1_d, \dots \beta^n_d) && \text{(naturalité de } \alpha_{x_0,x_1} \text{ en } x_1) \\
&= Ff \cdot \gamma_d \,. && \square
\end{aligned}$$

Il est possible, également, de voir la règle de coupure comme provenant d'une transformation naturelle, mais à condition de fixer un de ses deux arguments. En effet, étant donné une transformation naturelle $\beta : [\![C]\!] \to [\![B]\!]$, on peut définir la ***sémantique naturelle droite*** de la règle de coupure comme suit :

$$\begin{aligned}
[\mathtt{C}, \beta]_x : \mathcal{C}\big([\![A]\!](x_0)\ ,\ [\![C]\!](x_1)\big) &\to \mathcal{C}\big([\![A]\!](x_0)\ ,\ [\![B]\!](x_1)\big)\,, \\
h &\mapsto h \cdot \beta_{x_1}\,.
\end{aligned} \tag{4.1}$$

Alors la collection $[\mathtt{C}, \beta] = \big([\mathtt{C}, \beta]_x\big)_{x \in \overline{\mathcal{C}^V} \times \mathcal{C}^V}$ est une transformation naturelle de $\mathcal{C}([\![A]\!], [\![C]\!])$ vers $\mathcal{C}([\![A]\!], [\![B]\!])$: la démonstration de ce fait est identique à celle des règles $\mathtt{R}{+_i}$ et $\mathtt{RF}_X$ dans la Proposition 4.1.

De la même façon, étant donné $\beta : [\![A]\!] \to [\![C]\!]$ naturelle, la ***sémantique naturelle gauche*** de la règle de coupure est définie comme suit :

$$\begin{aligned} [\beta, \mathtt{C}]_x : \mathcal{C}\big([\![C]\!](x_0)\ ,\ [\![B]\!](x_1)\big) &\to \mathcal{C}\big([\![A]\!](x_0)\ ,\ [\![B]\!](x_1)\big)\ , \\ h &\mapsto \beta_{x_0} \cdot h\ . \end{aligned} \tag{4.2}$$

4.2 Adéquation

Dans cette section, on démontre que pour chaque preuve circulaire Π et chaque catégorie μ-bicomplète $\mathcal{C}$, on peut faire correspondre, à chaque sommet de Π, une flèche de $\mathcal{C}_V$ de façon à ce que les relations dictées par les règles du Tableau 3.2 soient satisfaites partout. C'est-à-dire qu'on considère la preuve Π comme déterminant un système d'équations qu'on cherche à résoudre, dont les variables sont les sommets de Π et les équations sont de la forme

$$\text{« } u = [\![\textsc{Règ}(u)]\!](v_1 \dots v_n) \text{ »} \quad (v_i \in \mathrm{suc}(u)) \tag{4.3}$$

pour chaque sommet $u \in \Pi$ tel que $\textsc{Règ}(u) \neq \mathtt{H}$. Pour y parvenir, on généralise la méthode utilisée dans (Santocanale, 2002a), où les règles d'identité et de coupure ne faisaient pas partie du système. Afin d'alléger les notations dans la présente section, étant donné une pré-preuve Π et un sommet $u \in \Pi$, on écrira $A_u = [\![\textsc{Seq}_{\mathtt{L}}(u)]\!]$ et $B_u = [\![\textsc{Seq}_{\mathtt{R}}(u)]\!]$.

Introduisons d'abord quelques notations relatives aux hypothèses. Étant donné une pré-preuve circulaire Π, soit $H_\Pi := \{u \in \Pi : \textsc{Règ}(u) = \mathtt{H}\}$ et C_Π le sous-graphe sont le support est $\Pi \setminus A_\Pi$, avec toutes les transitions de Π entre ses sommets. Les éléments de H_Π s'appellent les ***hypothèses*** de Π et ceux de C_Π sont ses ***conclusions***. On dit que Π est ***close*** si $H_\Pi = \varnothing$.

Définition. Soit Π une pré-preuve de $\mathbf{C}_{\mathcal{S}}$. Pour chaque $u \in C_\Pi$, soit

$$e_u = \mathtt{pr}^{\Pi}_{\mathrm{suc}(u)} \cdot [\![\mathrm{R\grave{E}G}(u)]\!] : \prod_{v \in C_\Pi} \mathcal{C}_V(A_v, B_v) \times \prod_{v \in H_\Pi} \mathcal{C}_V(A_v, B_v) \to \mathcal{C}_V(A_u, B_u).$$

Le ***système d'équations associé à*** Π est la fonction suivante :

$$[\![?\Pi]\!] = \langle e_v \rangle_{v \in C_\Pi} : \prod_{v \in C_\Pi} \mathcal{C}_V(A_v, B_v) \times \prod_{v \in H_\Pi} \mathcal{C}_V(A_v, B_v) \to \prod_{v \in C_\Pi} \mathcal{C}_V(A_v, B_v). \quad (4.4)$$

Une ***solution*** de $[\![?\Pi]\!]$ est une fonction

$$[\![!\Pi]\!] : \prod_{v \in H_\Pi} \mathcal{C}_V(A_v, B_v) \to \prod_{v \in C_\Pi} \mathcal{C}_V(A_v, B_v)$$

telle que pour tout vecteur $\vec{f} = (f_v)_{v \in H_\Pi}$ de transformations naturelles de la forme $f_v : A_v \to B_v$, on a

$$[\![!\Pi]\!](\vec{f}) = [\![?\Pi]\!]\big([\![!\Pi]\!](\vec{f}), \vec{f}\big).$$

On dit que Π est ***résoluble*** si $[\![?\Pi]\!]$ admet une solution. À ce moment là, pour tout $u \in \Pi$, la ***solution en*** u est définie comme suit :

$$[\![u]\!]_\Pi : \prod_{v \in H_\Pi} \mathcal{C}_V(A_v, B_v) \to \mathcal{C}_V(A_u, B_u)$$

$$\vec{f} \mapsto \begin{cases} \mathtt{pr}^{H_\Pi}_u(\vec{f}) & \text{si } u \in H_\Pi, \\ [\![!\Pi]\!](\vec{f}) \cdot \mathtt{pr}^{C_\Pi}_u & \text{si } u \in C_\Pi. \end{cases}$$

Il est immédiat de constater qu'étant donné une telle solution, pour chaque $u \in C_\Pi$, on a

$$[\![u]\!]_\Pi = [\![\mathrm{R\grave{E}G}(u)]\!] \circ \langle [\![v]\!]_\Pi \rangle_{v \in \mathrm{suc}(u)}$$

comme en (4.3). Réciproquement, étant donné une collection $\{[\![u]\!]_\Pi\}_{u \in C_(\Pi)}$ satisfaisant cette dernière équation, on peut retrouver une solution à $[\![?\Pi]\!]$ en posant

$$[\![!\Pi]\!] = \langle [\![u]\!]_\Pi \rangle_{u \in C_\Pi}.$$

Notre objectif est de démontrer que chaque preuve circulaire est résoluble. Le premier pas dans cette direction est de considérer les preuves *homogènes*.

Définition. Une preuve circulaire Π est ***homogène*** si elle ne contient pas d'instances de la règle $\mathtt{I}$ et si, pour toute coupure $u \in \Pi$, ou bien $\varsigma_0 u \in H_\Pi$ (auquel cas on pose $\chi_u = 0$), ou bien $\varsigma_1 u \in H_\Pi$ (auquel cas $\chi_u = 1$ s'il n'est pas déjà défini).

L'avantage des preuves homogènes est qu'on peut fixer la valeur d'un des successeurs de chaque coupure et, ainsi, exploiter la naturalité de la règle de coupure telle que décrite aux équations (4.1) et (4.2). Soit donc Π une preuve circulaire homogène. En supposant, sans perte de généralité, que chaque $u \in H_\Pi$ a un seul prédécesseur dans le graphe de Π, on peut séparer l'ensemble des hypothèses en deux parties :

$$H_\Pi^{\mathtt{c}} := \{\varsigma_{\chi_u} u \in H_\Pi : \text{RÈG}(u) = \mathtt{C}\} \quad \text{et} \quad H_\Pi^{\mathtt{s}} := H_\Pi \setminus H_\Pi^{\mathtt{c}} \,.$$

Enfin, pour chaque $u \in H_\Pi^{\mathtt{c}}$, fixons une transformation naturelle $\beta^u : A_u \to B_u$.

On définit le ***système naturel d'équations*** $[?^\beta \Pi]$ de façon analogue à $[\![?\Pi]\!]$. Pour chaque $u \in C_\Pi$ soit

$$\epsilon_u = \mathtt{pr}^{C_\Pi \cup H_\Pi^{\mathtt{s}}}_{\mathrm{suc}^\beta(u)} \cdot [\text{RÈG}^\beta(u)] : \prod_{v \in C_\Pi} \mathcal{C}(A_v, B_v) \times \prod_{v \in H_\Pi^{\mathtt{s}}} \mathcal{C}(A_v, B_v) \to \mathcal{C}(A_u, B_u)$$

où $[\text{RÈG}^\beta(u)] : \prod_{v \in \mathrm{suc}^\beta(u)} \mathcal{C}(A_v, B_v) \to \mathcal{C}(A_u, B_u)$ est défini comme suit :

- si $\text{RÈG}(u) \neq \mathtt{C}$, alors $\mathrm{suc}^\beta(u) = \mathrm{suc}(u)$ et $[\text{RÈG}^\beta(u)] = [\text{RÈG}(u)]$, comme dans la Proposition 4.1 ;
- si $\text{RÈG}(u) = \mathtt{C}$ et $\chi_v = 0$, alors $\mathrm{suc}^\beta(u) = \{\varsigma_0 u\}$ et $[\text{RÈG}^\beta(u)] = [\mathtt{C}, \beta^{\varsigma_1 u}]$, comme dans l'équation (4.1) ;
- si $\text{RÈG}(u) = \mathtt{C}$ et $\chi_v = 1$, alors $\mathrm{suc}^\beta(u) = \{\varsigma_1 u\}$ et $[\text{RÈG}^\beta(u)] = [\beta^{\varsigma_0 u}, \mathtt{C}]$, comme dans l'équation (4.2).

Une ***solution naturelle*** de $[?^\beta \Pi]$ est une transformation naturelle

$$[!^\beta \Pi] : \prod_{v \in H_\Pi^{\mathtt{s}}} \mathcal{C}(A_v, B_v) \to \prod_{v \in C_\Pi} \mathcal{C}(A_v, B_v)$$

telle que pour tout $x = (\overline{x_0}, x_1) \in \overline{\mathcal{C}^V} \times \mathcal{C}^V$ et $\vec{f} \in \prod_{v \in H^{\mathtt{s}}_\Pi} \mathcal{C}(A_v(x_0), B_v(x_1))$, on ait

$$[!^\beta \Pi]_x(\vec{f}) = [?^\beta \Pi]_x([!^\beta \Pi]_x(\vec{f}), \vec{f}).$$

Similairement à la définition de $[\![u]\!]_\Pi$, si $[?^\beta \Pi]$ admet une solution naturelle, on définit :

$$[^\beta u]_\Pi : \prod_{v \in H^{\mathtt{s}}_\Pi} \mathcal{C}(A_v, B_v) \to \mathcal{C}(A_u, B_u)$$

$$[^\beta u]_\Pi = \begin{cases} \mathtt{pr}_u^{H_\Pi} & \text{si } u \in H^{\mathtt{s}}_\Pi, \\ [!^\beta \Pi] \cdot \mathtt{pr}_u^{C_\Pi} & \text{si } u \in C_\Pi. \end{cases}$$

Alors étant donné une telle solution, pour chaque $u \in C_\Pi$, on a

$$[^\beta u]_\Pi = \langle [^\beta v]_\Pi \rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}^\beta(u)] \,.$$

Réciproquement, étant donné une collection $\{[^\beta u]_\Pi\}_{u \in C_(\Pi)}$ satisfaisant cette dernière équation, on peut retrouver une solution à $[\![?\Pi]\!]$ en posant

$$[!^\beta \Pi] = \langle [^\beta u]_\Pi \rangle_{u \in C_\Pi} \,.$$

Enfin, même si le système dirigé d'équations sous-jacent à Π était, jusque là, sous-entendu, il y aura lieu, dans la démonstration du prochain résultat, d'interpréter des preuves circulaires selon différents systèmes. Ainsi, lorsqu'il sera nécessaire de mentionner le système $\mathcal{S}$ sur lequel une preuve sera définie, on écrira explicitement $[?^\beta \Pi]^{\mathcal{S}}$ et $[!^\beta \Pi]^{\mathcal{S}}$, en plus de la convention établie à la fin de la Section 2.4.

Proposition 4.3. *Soit $\mathcal{S}$ un système dirigé d'équations et Π une preuve circulaire homogène sur $\mathcal{S}$. Pour chaque collection $\vec{\beta} = (\beta_v : A_v^{\mathcal{S}} \to B_v^{\mathcal{S}})_{v \in U}$ de transformations naturelles, où $H^{\mathtt{c}}_\Pi \subseteq U$, le système $[?^\beta \Pi]^{\mathcal{S}}$ admet une unique solution naturelle.*

Démonstration. On procède par récurrence (dans $\mathbb{N}^2$, qui est bien ordonné) sur la ***complexité*** de Π, définie comme suit :

$$\sharp(\Pi) = \left(\sharp_{\mathtt{L}}(\Pi) + \sharp_{\mathtt{R}}(\Pi),\, |C_\Pi| \right) \in \mathbb{N}^2 \,,$$

où $|C_\Pi|$ est la cardinalité de C_Π et, pour $\mathtt{D} \in \{\, \mathtt{L}, \mathtt{R} \,\}$,

$$\sharp_{\mathtt{D}}(\Pi) = \max\{p_X : \exists v \in \Pi \text{ t.q. } \text{RÈG}(v) = \mathtt{DF}_X\}.$$

Remarquons d'abord que si $\sharp_{\mathtt{L}}(\Pi)+\sharp_{\mathtt{R}}(\Pi) = 0$, alors Π est acyclique. On peut donc facilement résoudre $[\mathbf{?}^\beta \Pi]^{\mathcal{S}}$ en propageant la solution à partir des feuilles jusqu'à la racine de Π. Aussi, si $|C_\Pi| = 0$, alors le résultat est trivial puisque le codomaine de $[\mathbf{?}\Pi_\beta]^{\mathcal{S}}$ et de $[\mathbf{!}\Pi_\beta]^{\mathcal{S}}$ est l'objet terminal.

Dans les autres cas, on argumente selon que C_Π est fortement connexe ou non. Pour tout ensemble E, soit $\vec{E}$ le vecteur $\langle e \rangle_{e \in E}$. On cherche donc une solution en $\vec{C}_\Pi$ de l'équation suivante :

$$\vec{C}_\Pi = [\mathbf{?}^\beta \Pi]^{\mathcal{S}}(\vec{C}_\Pi, \vec{H}^{\mathtt{S}}_\Pi) \,. \tag{4.5}$$

Supposons que C_Π n'est pas fortement connexe. On a donc donc $v_1, v_2 \in C_\Pi$ tels qu'il n'existe aucun chemin de v_1 vers v_2. Soit Π_1 le plus grand sous-graphe accessible à partir de v_1 et soit $\Pi_2 = \langle |\Pi|, \text{SEQ}, \text{RÈG}' \rangle$, où $\text{RÈG}'(u) = \mathtt{H}$ si $u \in \Pi_1$ et $\text{RÈG}'(u) = \text{RÈG}(u)$ sinon. Alors on peut décomposer l'équation (4.5) en deux sous-problèmes :

$$\left\{ \begin{array}{l} \vec{C}_{\Pi_1} = [\mathbf{?}^\beta \Pi_1]^{\mathcal{S}}(\vec{C}_{\Pi_1}, \vec{H}^{\mathtt{S}}_{\Pi_1}) \\ \vec{C}_{\Pi_2} = [\mathbf{?}^\beta \Pi_2]^{\mathcal{S}}(\vec{C}_{\Pi_2}, \vec{C}_{\Pi_1}, \vec{H}^{\mathtt{S}}_{\Pi}) \end{array} \right\} . \tag{4.6}$$

Clairement, on a $|C_{\Pi_1}| < |C_\Pi|$ et $|C_{\Pi_2}| < |C_\Pi|$. Par hypothèse d'induction, on peut donc résoudre (4.6). Par le Lemme de Bekić (Lemme 2.3), on peut conclure que (4.5) admet une solution unique.

Supposons maintenant que C_Π est fortement connexe. Par la condition **G3**, C_Π a soit une μ-trace gauche, soit une ν-trace droite. On fait le reste de la démonstration en supposant que C_Π a une μ-trace gauche : une argumentation duale suffit à démontrer l'autre possibilité. Soit $m = \sharp_{\mathtt{L}}(\Pi)$ et posons

$$M = \{\, v \in C_\Pi : \text{RÈG}(v) = \mathtt{LF}_X \text{ et } p_X = m \,\}\,.$$

On commence par définir un système dirigé d'équations : $\mathcal{S}'$ et $\mathcal{T}$. Pour tout $X \in \mathsf{BV}(\mathcal{S})$, fixons une variable $X' \notin V \cup \mathsf{BV}(\mathcal{S})$. Pour toute formule φ, on définit la formule φ' par récurrence comme suit :

– si $\varphi = X \in \mathsf{BV}(\mathcal{S})$, alors $\varphi' = X'$;
– si $\varphi \in \{0, 1\}$ ou $\varphi = X \in \mathbb{V} \setminus \mathsf{BV}(\mathcal{S})$, alors $\varphi' = \varphi$;
– si $\varphi = \varphi_0 + \varphi_1$, alors $\varphi' = \varphi'_0 + \varphi'_1$;
– si $\varphi = \varphi_0 \times \varphi_1$, alors $\varphi' = \varphi'_0 \times \varphi'_1$.

Le système $\mathcal{S}'$ est simplement une copie de $\mathcal{S}$ dans lequel toutes les variables X sont substituées par X'. Formellement. $\mathcal{S}' = \langle B', F', p' \rangle$, où

$$\begin{aligned} B' &= \{X' : X \in \mathsf{BV}(\mathcal{S})\}\,, \\ p'_{X'} &= p_X\,, \\ F'_{X'} &= (F_X)'\,. \end{aligned}$$

Il est aisé de voir (par récurrence sur $\mathcal{S}$) que pour toute formule φ sans occurrences des variables de B', on a

$$[\![\varphi]\!]^{\mathcal{S}} = [\![\varphi']\!]^{\mathcal{S}'} : \mathcal{C}^V \to \mathcal{C}\,.$$

Quant au système $\mathcal{T}$, il s'agit d'une construction similaire au système prédécesseur de $\mathcal{S}$, mais par rapport à Π. On pose $\mathsf{BV}(\mathcal{T}) = \{X \in \mathsf{BV}(\mathcal{S}) : p_X < m\}$ et les priorités (p) ainsi que les formules associées (F) sont les mêmes que dans $\mathcal{S}$, mais restreintes à $\mathsf{BV}(\mathcal{T})$. Soit $W = \{X : X \in \mathsf{BV}(\mathcal{S}) \text{ et } p_X \geq m\}$. Alors, de façon similaire au Lemme 2.8, pour toute formule φ, il existe un isomorphisme naturel

$$\eta : [\![\varphi]\!]^{\mathcal{S}} \to [\![\varphi]\!]^{\mathcal{T}}(\vec{X}, \mathtt{id}),$$

où $\vec{X} = \langle [\![X]\!]^{\mathcal{S}}_V \rangle_{X \in W}$, et cet isomorphisme est l'identité si $\varphi = X \in W$.

Soit $\Pi' = \langle |\Pi|, \text{RÈG}', \text{SEQ}' \rangle$ la preuve circulaire sur le système $\mathcal{T} \cup \mathcal{S}'$ telle que, pour tout $u \in |\Pi|$,

– si $\text{SEQ}(u) = A \vdash B$, alors $\text{SEQ}'(u) = A \vdash B'$;

– si $u \in M$, alors $\text{RÈG}'(u) = \mathtt{H}$;

– si $\text{RÈG}(u) = \mathtt{RF}_X$, alors $\text{RÈG}'(u) = \mathtt{RF}_{X'}$;

– autrement, $\text{RÈG}'(u) = \text{RÈG}(u)$.

Alors par construction, les formules à gauche des séquents de Π' ne dépendent pas des variables de $\mathsf{BV}(\mathcal{S}')$ et celles à droite ne dépendent pas de celles de $\mathsf{BV}(\mathcal{S})$. Ainsi, pour tout $u \in \Pi'$, si on pose $\vec{\mathbf{1}} = \mathbf{1}^W$, on a les égalités suivantes

$$\begin{aligned} A^{\mathcal{T}}_u = A^{\mathcal{T}\cup\mathcal{S}'}_u &: \mathcal{C}^W \times \mathcal{C}^V \to \mathcal{C}\,, \\ {B'}^{\mathcal{S}'}_u = {B'}^{\mathcal{T}\cup\mathcal{S}'}_u(\vec{\mathbf{1}}, \mathtt{id}) &: \mathcal{C}^V \to \mathcal{C}\,, \\ {B'}^{\mathcal{T}\cup\mathcal{S}'}_u = \mathtt{pr}^{W\cup V}_V \cdot {B'}^{\mathcal{S}'}_u &: \mathcal{C}^W \times \mathcal{C}^V \to \mathcal{C}\,. \end{aligned}$$

Remarquons, de plus, que Π' est homogène, avec $H^{\mathtt{c}}_{\Pi'} = H^{\mathtt{c}}_{\Pi}$ et $H^{\mathtt{s}}_{\Pi'} = M \cup H^{\mathtt{s}}_{\Pi}$. De plus, puisque Π a une μ-trace gauche, alors pour tout $v \in H^{\mathtt{c}}_{\Pi'}$, il existe une coupure $u \in \Pi'$ telle que $v = \varsigma_1 u$. Ainsi, étant donné une collection $\vec{\beta} = (\beta_v : A^{\mathcal{S}}_v \to B^{\mathcal{S}}_v)_{v \in U}$ de transformations naturelles, où $H^{\mathtt{c}}_{\Pi} \subseteq U$ comme en hypothèse, soit $\vec{\beta}' = (\beta'_v : {A'}^{\mathcal{T}\cup\mathcal{S}'}_v \to {B'}^{\mathcal{T}\cup\mathcal{S}'}_v)_{v \in U}$ où , pour tout $(x, y) \in \mathcal{C}^W \times \mathcal{C}^V$, on pose $\beta'_{v;(x,y)} = \beta_{v;y}$. Remarquons enfin que, par construction, on a $\sharp_{\mathtt{R}}(\Pi') = \sharp_{\mathtt{R}}(\Pi)$ et $\sharp_{\mathtt{L}}(\Pi') < m = \sharp_{\mathtt{L}}(\Pi)$. Par l'hypothèse d'induction, le système $[?^{\beta'}\Pi']^{\mathcal{T}\cup\mathcal{S}}$ admet donc une solution unique :

$$[!^{\beta'}\Pi']^{\mathcal{T}\cup\mathcal{S}'} : \prod_{v\in M} \mathcal{C}(A^{\mathcal{T}\cup\mathcal{S}'}_v, {B'}^{\mathcal{T}\cup\mathcal{S}'}_v) \times \prod_{v\in H^{\mathtt{s}}_{\Pi}} \mathcal{C}(A^{\mathcal{T}\cup\mathcal{S}'}_v, {B'}^{\mathcal{T}\cup\mathcal{S}'}_v) \to \prod_{v\in C_{\Pi'}} \mathcal{C}(A^{\mathcal{T}\cup\mathcal{S}'}_v, {B'}^{\mathcal{T}\cup\mathcal{S}'}_v).$$

Pour tout $u \in M$, soit X_u la variable telle que $\text{RÈG}(u) = \mathtt{LF}_{X_u}$. Remarquons qu'on a $\varsigma u \in C_{\Pi}$, puisque C_{Π} est fortement connexe et ςu est l'unique successeur de u dans Π. De plus, on peut supposer sans perte de généralité que F_X n'est pas une

formule composée seulement d'une variable et donc, que $\text{RÈG}(\varsigma u) \neq \mathtt{LF}_X$, pour $X \in \mathsf{BV}(\mathcal{S})$. On en conclut que $\varsigma u \in C_{\Pi'}$. De plus, toujours pour $u \in M$, on a $A_u^{\mathcal{T}\cup\mathcal{S}} = A_u^{\mathcal{T}} = [\![X_u]\!]^{\mathcal{T}}$, $B_u^{\mathcal{S}} = B_{\varsigma u}^{\mathcal{S}}$ et $A_{\varsigma u}^{\mathcal{T}} = [\![F_{X_u}]\!]^{\mathcal{T}}$.

Soit ϑ la transformation naturelle en $x \in \mathcal{C}^W$, $y \in \mathcal{C}^V$ et $z \in \mathcal{C}^V$ définie par l'équation $\vartheta_{x,y,z} = [\mathbf{!}^{\beta}\Pi']^{\mathcal{T}\cup\mathcal{S}}_{x,y,\vec{\mathbf{1}},z} \cdot \mathtt{pr}^{C_{\Pi'}}_{\varsigma M}$. Le type de $\vartheta_{x,y,z}$ est donc le suivant :

$$\prod_{u\in M} \mathcal{C}\big([\![X_u]\!]^{\mathcal{T}}(x), {B'}_u^{\mathcal{S}'}(z)\big) \times \prod_{u\in H^{\mathbf{s}}_{\Pi}} \mathcal{C}\big(A_u^{\mathcal{T}}(x,y), {B'}_u^{\mathcal{S}'}(z)\big) \to \prod_{u\in M} \mathcal{C}\big([\![F_{X_u}]\!]^{\mathcal{T}}(x,y), {B'}_u^{\mathcal{S}'}(z)\big).$$

Or, rappelons que pour tout u, on a ${B'}_u^{\mathcal{S}'} = B_u^{\mathcal{S}}$. Pour tout $X \in W$, soit

$$\widetilde{B}_X^{\mathcal{S}} := \prod_{u\in M, X_u = X} {B'}_u^{\mathcal{S}'} = \prod_{u\in M, X_u = X} B_u^{\mathcal{S}}.$$

On définit deux isomorphismes naturels comme suit :

$$\begin{aligned}
\sigma : \prod_{u\in M} \mathcal{C}\big([\![X_u]\!]^{\mathcal{T}}, B_u^{\mathcal{S}}\big) &\xrightarrow{\sim} \prod_{X\in W} \prod_{u\in M, X_u = X} \mathcal{C}\big([\![X_u]\!]^{\mathcal{T}}, B_u^{\mathcal{S}}\big) \\
&= \prod_{X\in W} \prod_{u\in M, X_u = X} \mathcal{C}\big([\![X]\!]^{\mathcal{T}}, B_u^{\mathcal{S}}\big) \\
&\xrightarrow{\sim} \prod_{X\in W} \mathcal{C}\big([\![X]\!]^{\mathcal{T}}, \widetilde{B}_X^{\mathcal{S}}\big)
\end{aligned}$$

et, de façon similaire :

$$\begin{aligned}
\tau : \prod_{u\in M} \mathcal{C}\big([\![F_{X_u}]\!]^{\mathcal{T}}, B_u^{\mathcal{S}}\big) &\xrightarrow{\sim} \prod_{X\in W} \prod_{u\in M, X_u = X} \mathcal{C}\big([\![F_{X_u}]\!]^{\mathcal{T}}, B_u^{\mathcal{S}}\big) \\
&= \prod_{X\in W} \prod_{u\in M, X_u = X} \mathcal{C}\big([\![F_X]\!]^{\mathcal{T}}, B_u^{\mathcal{S}}\big) \\
&\xrightarrow{\sim} \prod_{X\in W} \mathcal{C}\big([\![F_X]\!]^{\mathcal{T}}, \widetilde{B}_X^{\mathcal{S}}\big).
\end{aligned}$$

Or, $\forall X \in W$, on a $[\![X]\!]^{\mathcal{T}} = \mathtt{pr}^W_X$. Soit $\vartheta' = (\sigma^{-1} \times \mathtt{id}) \cdot \vartheta \cdot \tau$. Alors le type de $\vartheta'_{x,y,z}$ est le suivant :

$$\prod_{X\in W} \mathcal{C}\big(\mathtt{pr}_X(x), \widetilde{B}_X^{\mathcal{S}}(z)\big) \times \prod_{u\in H^{\mathbf{s}}_{\Pi}} \mathcal{C}\big(A_u^{\mathcal{T}}(x,y), B_u^{\mathcal{S}}(z)\big) \to \prod_{x\in W} \mathcal{C}\big([\![F_X]\!]^{\mathcal{T}}(x,y), \widetilde{B}_X^{\mathcal{S}}(z)\big).$$

Or, ϑ est une transformation naturelle de la forme exigée par le Corollaire 2.5, qu'on instancie avec les foncteurs suivants :

$$\begin{aligned}
&F : \mathcal{C}^W \times \mathcal{C}^V \to \mathcal{C}^W && , \quad F = \langle [\![F_X]\!]^{\mathcal{T}} \rangle_{X \in W} \; ; \\
&Q : \overline{\mathcal{C}^W} \times \overline{\mathcal{C}^V} \times \mathcal{C}^V \to \mathcal{E}\mathit{ns} && , \quad Q(x,y,z) = \prod_{u \in H_\Pi^{\mathrm{s}}} \mathcal{C}\big(A_u^{\mathcal{T}}(x,y), B_u^{\mathcal{S}}(z)\big) \; ; \\
&T_X : \mathcal{C}^V \to \mathcal{C} && , \quad T_X = \widetilde{B}_X^{\mathcal{S}} \qquad (\forall X \in W).
\end{aligned}$$

Notons que l'algèbre initiale paramétrée du foncteur F est la paire $(\vec{X}, \vec{\alpha})$, où $\vec{X} = \big\langle [\![X]\!]^{\mathcal{S}} \big\rangle_{X \in W}$ et $\vec{\alpha} = \prod_{X \in W} (\xi_X^{-1} \cdot \alpha_X)$ où

$$\xi_X : [\![F_X]\!]^{\mathcal{S}} \to [\![F_X]\!]^{\mathcal{T}}(\vec{X}, \mathtt{id})$$

est un isomorphisme naturel. Ainsi, pour tout $y, z \in \mathcal{C}^V$, on a

$$\begin{aligned}
Q(F^\mu(y), y, z) &= Q(\vec{X}(y), y, z) \\
&= \prod_{u \in H_\Pi^{\mathrm{s}}} \mathcal{C}\big(A_u^{\mathcal{T}}(\vec{X}(y), y), B_u^{\mathcal{S}}(z)\big) \\
&= \prod_{u \in H_\Pi^{\mathrm{s}}} \mathcal{C}\big(A_u^{\mathcal{S}}(y), B_u^{\mathcal{S}}(z)\big).
\end{aligned}$$

Ainsi, par le Corollaire 2.5, il existe une unique transformation naturelle

$$f : \prod_{v \in H_\Pi^{\mathrm{s}}} \mathcal{C}\big(A_v^{\mathcal{T}}(\vec{X}, \mathtt{id}), B_v^{\mathcal{S}}\big) \to \prod_{X \in W} \mathcal{C}\big([\![X]\!]^{\mathcal{S}}, \widetilde{B}_X^{\mathcal{S}}\big),$$

telle que $\forall y, z \in \mathcal{C}^V$ et tout choix d'élément $q \in \prod_{v \in H_\Pi} \mathcal{C}\big(A_v^{\mathcal{T}}(\vec{X}(y), y), B_v^{\mathcal{S}}(z)\big)$, on a :

$$\vec{\alpha}_y \cdot f_{y,z}(q) = \vartheta'_{\vec{X}(y), y, z}(f_{y,z}(q), q)\,. \tag{4.7}$$

Or, rappelons qu'on a un isomorphisme naturel :

$$\delta = \sigma^{-1}_{\vec{X}, \mathtt{id}} : \prod_{X \in W} \mathcal{C}\big([\![X]\!]^{\mathcal{S}}, \widetilde{B}_X^{\mathcal{S}}\big) \to \prod_{u \in M} \mathcal{C}\big([\![X_u]\!]^{\mathcal{S}}, B_u^{\mathcal{S}}\big).$$

Ainsi, pour tout $u \in M$, on définit $h_u = f \cdot \delta \cdot \mathtt{pr}_u$. On étend cette solution potentielle à tous les $u \in C_{\Pi'}$ de la façon suivante. On définit h_u par la composition suivante :

$$\prod_{v \in H^{\mathtt{S}}_{\Pi}} \mathcal{C}\big(A^{\mathcal{T}}_v(\vec{X}, \mathtt{id}), B^{\mathcal{S}}_v\big) \xrightarrow{\langle f \cdot \delta \,,\, \mathtt{id}\rangle} \prod_{v \in M} \mathcal{C}\big([\![X_v]\!]^{\mathcal{S}}, B^{\mathcal{S}}_v\big) \times \prod_{v \in H^{\mathtt{S}}_{\Pi'}} \mathcal{C}\big(A^{\mathcal{T}}_v(\vec{X}, \mathtt{id}), B^{\mathcal{S}}_v\big)$$
$$\xrightarrow{[^{\beta'}u]^{\mathcal{T}\cup\mathcal{S}'}_{\Pi';(\vec{X},\_,\vec{\mathbf{i}},\_)}} \mathcal{C}\big(A^{\mathcal{T}}_u(\vec{X}, \mathtt{id}), B^{\mathcal{S}}_u\big)\,.$$

Enfin, pour tout $v \in \Pi$, soit

$$\eta_v : A^{\mathcal{S}}_v \xrightarrow{\sim} A^{\mathcal{T}}_v(\vec{X}, \mathtt{id}).$$

On pose $[^{\beta}u]^{\mathcal{S}}_{\Pi} = \eta_u \cdot h_u\big(\vec{\eta}\big)$. On a donc

$$[^{\beta}u]^{\mathcal{S}}_{\Pi} : \prod_{v \in H^{\mathtt{S}}_{\Pi}} \mathcal{C}(A^{\mathcal{S}}_v, B^{\mathcal{S}}_v) \to \mathcal{C}(A^{\mathcal{S}}_u, B^{\mathcal{S}}_u)\,.$$

Il ne reste qu'à vérifier qu'il s'agit d'une solution, c'est-à-dire que pour tout $u \in \Pi$, on a

$$[^{\beta}u]^{\mathcal{S}}_{\Pi} = [\mathrm{R\grave{E}G}^{\beta}(u)]^{\mathcal{S}}\big(\langle [^{\beta}v]^{\mathcal{S}}_{\Pi}\rangle_{v \in \mathrm{suc}(u)}\big).$$

Si $u \in C_{\Pi} \setminus M$, alors on a :

$$\begin{aligned}
[^{\beta}u]^{\mathcal{S}}_{\Pi} &= \eta_u \cdot h_u(\vec{\eta}) \\
&= \eta_u \cdot \Big(\big(\langle f \cdot \delta \,,\, \mathtt{id}\rangle \cdot [^{\beta'}u]^{\mathcal{T}\cup\mathcal{S}'}_{\Pi';(\vec{X},_,\vec{\mathbf{i}},_)}\big)(\vec{\eta})\Big) \\
&= \eta_u \cdot \Big(\langle f \cdot \delta \,,\, \mathtt{id}\rangle \cdot \big\langle [^{\beta'}v]^{\mathcal{T}\cup\mathcal{S}'}_{\Pi';(\vec{X},_,\vec{\mathbf{i}},_)}(\vec{\eta})\big\rangle_{v \in \mathrm{suc}(u)}\Big) \cdot [\mathrm{R\grave{E}G}^{\beta}(u)]^{\mathcal{T}\cup\mathcal{S}'} \\
&= \Big\langle \eta_u \cdot \big(\langle f \cdot \delta \,,\, \mathtt{id}\rangle \cdot [^{\beta'}v]^{\mathcal{T}\cup\mathcal{S}'}_{\Pi';(\vec{X},_,\vec{\mathbf{i}},_)}(\vec{\eta})\big)\Big\rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}^{\beta}(u)]^{\mathcal{T}\cup\mathcal{S}'} \\
&= \langle [v]^{\mathcal{S}}_{\Pi}\rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}^{\beta}(u)]^{\mathcal{S}}\,.
\end{aligned}$$

Si $u \in M$, on effectue plutôt la vérification suivante. Soit $\vec{X'} = \big\langle [\![X_u]\!]^{\mathcal{S}}\big\rangle_{u \in M}$ et $\vec{\alpha'} = \prod_{u \in M}(\xi^{-1}_{X_u} \cdot \alpha_{X_u})$ et

$$\varepsilon = \tau^{-1}_{\vec{X},\mathtt{id}} :: \prod_{X \in W} \mathcal{C}\big([\![F_X]\!]^{\mathcal{T}}(\vec{X}, \mathtt{id}), \widetilde{B}^{\mathcal{S}}_X\big) \xrightarrow{\sim} \prod_{u \in M} \mathcal{C}\big([\![F_{X_u}]\!]^{\mathcal{T}}(\vec{X}, \mathtt{id}), B^{\mathcal{S}}_u\big).$$

Alors, clairement, pour tout $a \in \prod_{X \in W} \mathcal{C}\big([\![F_X]\!]^{\mathcal{T}}(\vec{X}y, y)\,,\, \widetilde{B}^{\mathcal{S}}_X(z)\big)$, on a

$$\delta_{y,z}(\vec{\alpha}_y^{-1} \cdot a) = \vec{\alpha}'^{-1}_y \cdot \varepsilon_{y,z}(a)\,,$$

Enfin, rappelons que, par le Lemme 2.8, on a $\eta_u = \mathtt{id}$. Alors :

$$\begin{aligned}
[^{\beta}u]^{\mathcal{S}}_{\Pi} &= \vec{\eta} \cdot h_u \cdot \eta_u^{-1} \\
&= \vec{\eta} \cdot f \cdot \delta \cdot \mathtt{pr}_u \\
&= \mathtt{pr}_u \circ \delta\big(\vec{\alpha}^{-1} \cdot \vartheta'_{\vec{X},_,_}(\vec{\eta} \cdot f, \vec{\eta})\big) \\
&= \mathtt{pr}_u\Big(\vec{\alpha}'^{-1} \cdot \varepsilon\big(\vartheta'_{\vec{X},_,_}(\vec{\eta} \cdot f, \vec{\eta})\big)\Big) \\
&= \alpha^{-1}_{X_u} \cdot \xi_{X_u} \cdot (\mathtt{pr}_u \circ \not\in)\Big(\vartheta_{\vec{X},_,_}(\vec{\eta} \cdot f \cdot \delta, \vec{\eta}) \cdot \not{\varepsilon}^{\mathcal{X}}\Big) \\
&= \alpha^{-1}_{X_u} \cdot \eta_{\varsigma u} \cdot \mathtt{pr}_u\Big(\langle \vec{\eta} \cdot f \cdot \delta, \vec{\eta}\rangle \cdot [\mathbf{!}^{\beta'}\Pi']^{\mathcal{T}\cup\mathcal{S}}_{\vec{X},_,\vec{\mathtt{i}},_} \cdot \mathtt{pr}^{C_{\Pi'}}_{\varsigma M}\Big) \\
&= \alpha^{-1}_{X_u} \cdot \eta_{\varsigma u} \cdot \mathtt{pr}_u\Big(\big\langle \vec{\eta} \cdot \langle f \cdot \delta, \mathtt{id}\rangle \cdot [^{\beta'}\varsigma v]^{\mathcal{T}\cup\mathcal{S}'}_{\Pi'\,\vec{X},_,_}\big\rangle_{v \in M}\Big) \\
&= \alpha^{-1}_{X_u} \cdot \eta_{\varsigma u} \cdot \Big(\vec{\eta} \cdot \langle f \cdot \delta, \mathtt{id}\rangle \cdot [^{\beta'}\varsigma u]^{\mathcal{T}\cup\mathcal{S}'}_{\Pi'\,\vec{X},_,_}\Big) \\
&= \alpha^{-1}_{X_u} \cdot \eta_{\varsigma u} \cdot \Big(h_{\varsigma u}(\vec{\eta})\Big) \\
&= \alpha^{-1}_{X_u} \cdot [^{\beta}\varsigma v]^{\mathcal{S}}_{\Pi} \\
&= [\mathtt{LF}^{\beta}_{X_u}]^{\mathcal{S}}\big([\varsigma^{\beta}u]^{\mathcal{S}}_{\Pi}\big)\,.
\end{aligned}$$

Réciproquement, toute solution au système $[\mathbf{?}^{\beta}\Pi]^{\mathcal{S}}$ engendre une solution à l'équation (6.1) en remontant le calcul, d'où on conclut qu'il y a unicité. □

Théorème 4.4 (Adéquation)**.** *Soit* Π *une preuve circulaire. Alors* Π *est résoluble.*

Démonstration. On doit montrer que le système d'équation $[\![\mathbf{?}\Pi]\!]$ associé à Π (revoir l'équation (4.4)) admet une unique solution. On procède par induction bien fondée sur l'ensemble $\mathcal{K}$ des composantes fortement connexes de Π. Pour ce faire, on ordonne $\mathcal{K}$ selon l'ordre $\leq$ dual à la relation $\Rightarrow$ de la Section 1.4 (voir

Proposition 1.12). On a donc

$$K \leq K' \iff \exists u \in K' \text{ et } v \in K \text{ tels que } u \twoheadrightarrow v.$$

Puisque Π est finie, alors $\mathcal{K}$ est un ensemble fini. La relation d'ordre $\leq$ est donc bien fondée. De plus, pour tout $v \in \Pi$, il existe une unique composante $K_v \in \mathcal{K}$ (possiblement triviale) telle que $v \in \mathcal{K}$: on peut la calculer en faisant un parcours en largeur de Π à partir du sommet v, puis en éliminant les sommets qui ne reviennent jamais à v.

Soit $K \in \mathcal{K}$. Alors il y a deux possibilités à considérer : K est une composante triviale ou non. Si K est une composante triviale, soit $u \in K$ son unique sommet. Alors pour tout $v \in \mathrm{suc}(u)$, on a $K_v < K$ et donc, par hypothèse d'induction, $[\![v]\!]_\Pi$ est bien défini. On pose alors

$$[\![u]\!]_\Pi = \begin{cases} \mathtt{pr}_u^{H_\Pi} & \text{si } \text{RÈG}(u) = \mathtt{H}\,; \\ [\![\text{RÈG}(u)]\!] \circ \langle [\![v]\!]_\Pi \rangle_{v \in \mathrm{suc}(u)} & \text{sinon.} \end{cases}$$

Supposons maintenant que K n'est pas triviale. Un *bourgeon* de K est un sommet $v \in \Pi \setminus K$ pour lequel $\exists u \in K$ tel que $u \to v$. Soit $\mathcal{B}$ l'ensemble des bourgeons de K. Notons que pour tout $v \in \mathcal{B}$, on a $K_v < K$ et donc, par l'hypothèse d'induction, $[\![v]\!]_\Pi$ est bien défini.

Soit la pré-preuve $\Pi_K = \langle K \cup \mathcal{B}, \text{RÈG}', \text{SEQ}\restriction_{K \cup \mathcal{B}} \rangle$, où

$$\text{RÈG}'(u) = \begin{cases} \mathtt{H} & \text{si } u \in \mathcal{B}\,; \\ \text{RÈG}(u) & \text{sinon.} \end{cases}$$

Clairement, Π_K est une pré-preuve finie et, puisque ses seuls sous-graphes fortement connexes non triviaux des parties de K, Π_K satisfait la condition de garde **G3**. Π_K est donc une preuve circulaire. De plus, K ne contient *aucune* hypothèse

de Π, car il n'y a aucun chemin non nul dans Π dont la source est une hypothèse. On a donc $H_{\Pi_K} = \mathcal{B}$ et $C_{\Pi_K} = K$. Enfin, Π_K est une preuve homogène car, par la condition de garde **G3**, toutes ses coupures sont du même côté (gauche ou droit). Il existe donc $i \in \{0, 1\}$ tel que pour toute coupure u de K, on ait $\varsigma_i u \in \mathcal{B} = H_{\Pi_K}$.

Soit $\beta = (\llbracket v \rrbracket_\Pi)_{v \in H_K^{\mathtt{c}}}$ (c'est bien défini car $H_K^{\mathtt{c}} \subseteq \mathcal{B}$). Par la Proposition 4.3, le système $[\mathbf{?}^\beta \Pi_K]$ admet une unique solution naturelle

$$[\mathbf{!}^\beta \Pi_K] \ : \prod_{v \in H^{\mathtt{s}}_{\Pi_K}} \mathcal{C}(A_v, B_v) \to \prod_{u \in K} \mathcal{C}(A_u, B_u) \ .$$

Soit $\vec{\eta} = \langle \llbracket v \rrbracket_\Pi \rangle_{v \in H^{\mathtt{s}}_{\Pi_K}}$. Pour tout $u \in K$, on pose alors $\llbracket u \rrbracket_\Pi = (\llbracket u \rrbracket_{\Pi;c})_{c \in \mathcal{C}^V}$ où

$$\llbracket u \rrbracket_{\Pi;c} := \vec{\eta}_c \cdot [\mathbf{!}^\beta \Pi_K]_{c,c} \cdot \mathtt{pr}_u^K \ .$$

Par le Lemme 4.2, $\llbracket u \rrbracket_\Pi$ est bel et bien une transformation naturelle

$$\llbracket u \rrbracket_\Pi : \prod_{v \in H_\Pi} \mathcal{C}_V(A_v, B_v) \to \mathcal{C}_V(A_u, B_u) \, .$$

Enfin, on a

$$\begin{aligned}
\llbracket u \rrbracket_{\Pi;c} &= \vec{\eta}_c \cdot [\mathbf{!}^\beta \Pi_K]_{c,c} \cdot \mathtt{pr}_u^K \\
&= \vec{\eta}_c \cdot \big([\mathbf{?}^\beta \Pi_K]([\mathbf{!}^\beta \Pi_K], \mathtt{id}) \big)_{c,c} \cdot \mathtt{pr}_u^K \\
&= \vec{\eta}_c \cdot \epsilon_{u;c,c} \big([\mathbf{!}^\beta \Pi_K]_{c,c}, \mathtt{id} \big) \\
&= \epsilon_{u;c,c} \big(\vec{\eta}_c \cdot [\mathbf{!}^\beta \Pi_K]_{c,c}, \vec{\eta}_c \big) \\
&= [\mathrm{R\grave{E}G}^\beta(u)]_{c,c} \circ \mathtt{pr}^{C_\Pi \cup H^{\mathtt{s}}_\Pi}_{\mathrm{suc}^\beta(u)} \big(\vec{\eta}_c \cdot [\mathbf{!}^\beta \Pi_K]_{c,c}, \vec{\eta}_c \big) \, .
\end{aligned}$$

On cherche à en conclure $\llbracket u \rrbracket_\Pi = \llbracket \mathrm{R\grave{E}G}(u) \rrbracket \circ \langle \llbracket v \rrbracket_\Pi \rangle_{v \in \mathrm{suc}(u)}$. Pour ce faire, on conditionne sur $\mathrm{R\grave{E}G}(u)$ comme suit.

– Si $\mathrm{R\grave{E}G}(u) \neq \mathtt{C}$, alors $\mathrm{suc}^\beta(u) = \mathrm{suc}(u)$ et $[\mathrm{R\grave{E}G}^\beta(u)] = [\mathrm{R\grave{E}G}(u)]$. En particulier, puisque $\llbracket \mathrm{R\grave{E}G}(u) \rrbracket$ et $[\mathrm{R\grave{E}G}(u)]$ sont définies de la même manière à partir du Tableau 3.2, on a

$$(\llbracket \mathrm{R\grave{E}G}(u) \rrbracket(\vec{f}))_c = [\mathrm{R\grave{E}G}(u)]_{c,c}(\vec{f}_c) \, .$$

pour tout $c \in \mathcal{C}^V$ et $\vec{f} \in \prod_{v\in\mathrm{suc}(u)} \mathcal{C}_V(A_v, B_v)$. De plus, pour tout $v \in \mathrm{suc}(u)$, si $v \in K$, on a

$$\mathtt{pr}_v^{C_\Pi \cup H^{\mathtt{s}}_\Pi}\big(\,\vec{\eta_c}\cdot[!^\beta \Pi_K]_{c,c}, \vec{\eta_c}\,\big) = \vec{\eta_c}\cdot[!^\beta\Pi_K]_{c,c}\cdot \mathtt{pr}_v^K = [\![v]\!]_{\Pi;c}\,.$$

Sinon, $v \in \mathcal{B}$ et, puisque u n'est pas une coupure, on a $v \in H^{\mathtt{s}}_{\Pi_K}$. On trouve donc

$$\mathtt{pr}_v^{C_\Pi \cup H^{\mathtt{s}}_\Pi}\big(\,\vec{\eta_c}\cdot[!^\beta \Pi_K]_{c,c}, \vec{\eta_c}\,\big) = \vec{\eta_c}\cdot \mathtt{pr}_v^{H^{\mathtt{s}}_{\Pi_K}} = [\![v]\!]_{\Pi;c}\,.$$

En mettant ces éléments ensemble, on trouve $[\![u]\!]_\Pi = [\![\mathrm{RÈG}(u)]\!] \circ \langle [\![v]\!]_\Pi\rangle_{v\in\mathrm{suc}(u)}$.

– Si u est une coupure gauche, alors $\mathrm{suc}^\beta(u) = \{\varsigma_0 u\}$ et $[\mathrm{RÈG}^\beta(u)] = [\mathtt{C}, \beta^{\varsigma_1 u}]$. Par définition de β, on obtient $[\mathrm{RÈG}^\beta(u)]_{c,c}(x) = x \cdot [\![\varsigma_1 u]\!]_{\Pi;c}$. De plus, puisque $\varsigma_0 u \in K$, alors comme plus haut,

$$\mathtt{pr}^{C_\Pi \cup H^{\mathtt{s}}_\Pi}_{\mathrm{suc}^\beta(u)}\big(\,\vec{\eta_c}\cdot[!^\beta \Pi_K]_{c,c}, \vec{\eta_c}\,\big) = \vec{\eta_c}\cdot[!^\beta\Pi_K]_{c,c}\cdot \mathtt{pr}_{\varsigma_0 u} = [\![\varsigma_0 u]\!]_{\Pi;c}\,.$$

On obtient donc

$$[\![u]\!]_{\Pi;c} = [\![\varsigma_0 u]\!]_\Pi \cdot [\![\varsigma_0 u]\!]_\Pi = [\![\mathtt{C}]\!]\big([\![\varsigma_0 u]\!]_\Pi, [\![\varsigma_0 u]\!]_\Pi\big)\,.$$

– Si u est une coupure droite, on procède de façon duale au cas gauche. □

4.3 Plénitude

L'ajout de la règle de coupure au système de Santocanale (2001) a certes complexifié la démonstration de l'adéquation des preuves circulaires, mais on y a aussi gagné quelque chose. En effet, le système sans coupures n'est pas *plein*, en ce sens qu'il existe certaines flèches qui *devraient* pouvoir être dénotées par des preuves circulaires alors que ce n'est pas le cas.

Considérons, par exemple, le système dirigé de la Figure 4.1. On y reconnaît, bien sûr, l'équation « $N =_\mu 1 + N$ » qui définit les nombres naturels (donc $[\![N]\!] = \mathbb{N}$).

On peut trouver $[M]$ de façon similaire, ou encore en invoquant le Théorème 2.10 : une stratégie gagnante de $J(\mathcal{S})$ à partir de M est décrite par un certain nombre (fini) de tours sur la boucle en M, suivi d'un certain nombre (encore fini) de tours de boucle en N, donc par une paire de nombres naturels, d'où $[\![M]\!] \cong \mathbb{N}^2$.

$$\mathcal{S} = \left\{ \begin{array}{lll} M & =_\mu & N + M \\ N & =_\mu & 1 + N \end{array} \right\} \quad \stackrel{J}{\longmapsto} \quad$$

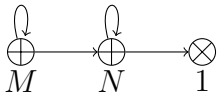


Figure 4.1 Un système représentant les paires de nombres naturels

La fonction diagonale $\Delta : \mathbb{N} \to \mathbb{N}^2$, qui envoie chaque $n \in \mathbb{N}$ sur la paire (n, n), peut être définie par induction comme suit :

$$\Delta(0) = (0, 0)\,,$$
$$\Delta(\texttt{Suc}\ n) = (\texttt{SucSuc})(\Delta(n))\,,$$

où $\texttt{SucSuc} : \mathbb{N}^2 \to \mathbb{N}^2$ est la fonction qui prend le successeur de chacune des deux coordonnées. C'est-à-dire que Δ satisfait le diagramme commutatif suivant :

$$\begin{array}{ccc} \mathbf{1} + \mathbb{N} & \xrightarrow{\mathbf{1}+\Delta} & \mathbf{1} + \mathbb{N}^2 \\ {\scriptstyle \alpha_N}\downarrow & & \downarrow{\scriptstyle \{(0,0),\texttt{SucSuc}\}} \\ \mathbb{N} & \xrightarrow[\Delta]{} & \mathbb{N}^2 \end{array} .$$

Or, puisque la fonction $\{(0, 0), \texttt{SucSuc}\}$ est définissable par une preuve circulaire sans coupures (essayez !) on serait en droit de s'attendre à ce que Δ le soit également. Ce n'est toutefois pas le cas.

Proposition 4.5 (Santocanale, 2001, Proposition 5.14)**.** *Il n'existe aucune preuve circulaire* ***sans coupures*** Π *telle que, pour un certain* $u \in \Pi$, $\textsc{Seq}(u) = N \vdash M$ *et* $[\![u]\!]_\Pi = \Delta$ *dans* $\mathcal{Ens}$.

La règle de coupure résout cette situation. En effet, la racine de la preuve qui se trouve à la Figure 4.2 dénote Δ. La construction de cette preuve a été faite en suivant la démonstration du Théorème 4.7 ci-dessous, qui exprime le phénomène général.

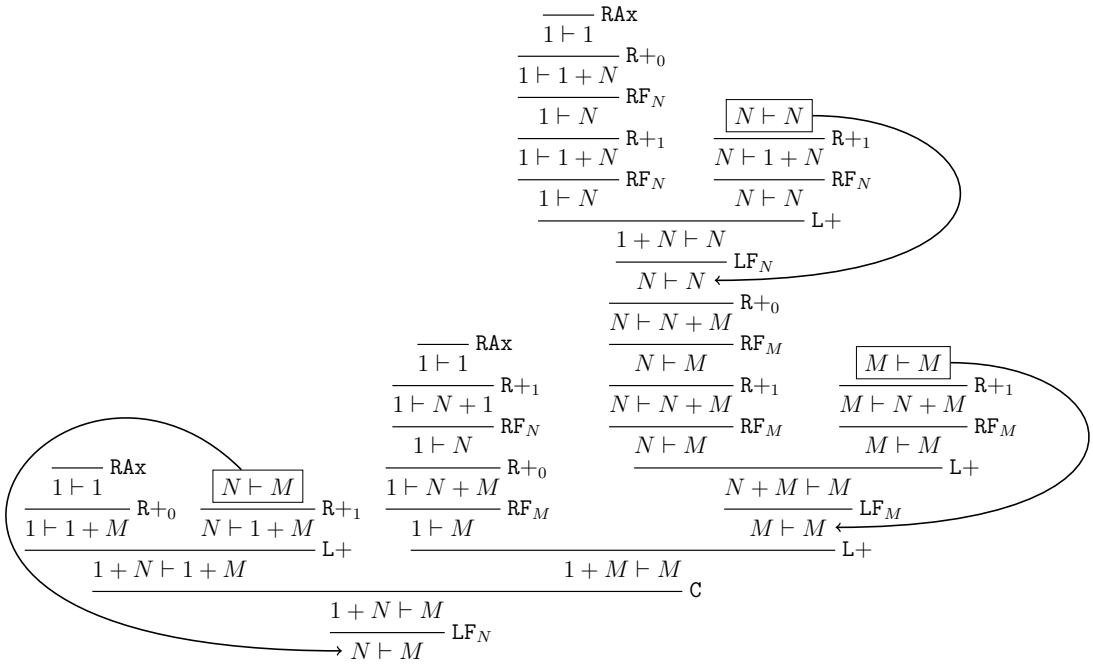


Figure 4.2 Une preuve circulaire dénotant la fonction diagonale

Lemme 4.6. *Soit $\mathcal{S}$ un système dirigé d'équations clos tel que $\mathsf{MAX}(\mathcal{S}) = \{X\}$ et soit $H = [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}$. Alors il existe une preuve circulaire sans coupures (et donc homogène) Γ et un sommet $u_0 \in \Gamma$ tels que $[u_0]_\Gamma^{\mathsf{P}(\mathcal{S})} : \mathcal{M}(\_,\_) \to \mathcal{M}(H,H)$ est la transformation naturelle canonique. C'est-à-dire que pour tout $x = (\overline{x_0}, x_1) \in \overline{\mathcal{C}^V} \times \mathcal{C}^V$ et $h \in \mathcal{C}(x_0, x_1)$, on a $[u_0]^{\mathsf{P}(\mathcal{S})}_{\Gamma;x_0,x_1}(h) = H(h)$.*

Démonstration. Comme dans la démonstration de la Proposition 4.3, on définit un système dirigé $\mathcal{S}'$ qui est une copie de $\mathcal{S}$ dans laquelle chaque variable $Y \in \mathsf{BV}(\mathcal{S})$ est remplacée par une nouvelle variable Y'. Rappelons que, par récurrence sur $\mathcal{S}$,

pour toute formule φ sans occurrences des variables de $\mathsf{BV}(\mathcal{S})$, on a

$$[\![\varphi]\!]^{\mathsf{P}(\mathcal{S})} = [\![\varphi']\!]^{\mathsf{P}(\mathcal{S}')}$$

où φ' est défini comme dans la Proposition 4.3. En particulier, on a

$$H = [\![F_X]\!]^{\mathsf{P}(\mathcal{S})} = [\![F'_{X'}]\!]^{\mathsf{P}(\mathcal{S})}.$$

Soit Γ la plus petite pré-preuve sur $\mathsf{P}(\mathcal{S}) \cup \mathsf{P}(\mathcal{S}')$ qui contient, au minimum, deux sommets distincts, u_0 et $u_{\mathtt{F}}$, tels que $\textsc{Seq}(u_0) = F_X \vdash (F_X)'$, $\textsc{Seq}(u_{\mathtt{F}}) = X \vdash X'$, $\textsc{Règ}(u_{\mathtt{F}}) = \mathtt{H}$, et telle que pour tout sommet $v \in \Gamma \setminus \{u_{\mathtt{F}}\}$ avec $\textsc{Seq}(v) = \varphi \vdash \varphi'$, les propriétés suivantes sont satisfaites :

– si $\varphi = 0$, alors $\textsc{Règ}(v) = \mathtt{LAx}$;

– si $\varphi = 1$, alors $\textsc{Règ}(v) = \mathtt{RAx}$;

– si $\varphi = Y \in \mathsf{BV}(\mathcal{S})$, alors le morceau de preuve suivant fait partie de Γ :

$$\dfrac{\dfrac{F_Y \vdash (F_Y)'}{F_Y \vdash Y'}\,\mathtt{RF}_{Y'}}{v : Y \vdash Y'}\,\mathtt{LF}_Y \quad ;$$

– si $\varphi = (\varphi_0 \times \varphi_1)$, alors le morceau de preuve suivant fait partie de Γ :

$$\dfrac{\dfrac{\varphi_0 \vdash \varphi'_0}{\varphi_0 \times \varphi_1 \vdash \varphi'_0}\,\mathtt{L}\times_0 \qquad \dfrac{\varphi_1 \vdash \varphi'_1}{\varphi_0 \times \varphi_1 \vdash \varphi'_1}\,\mathtt{L}\times_1}{v : \varphi_0 \times \varphi_1 \vdash \varphi'_0 \times \varphi'_1}\,\mathtt{R}\times \quad ;$$

– si $\varphi = (\varphi_0 + \varphi_1)$, alors le morceau de preuve suivant fait partie de Γ :

$$\dfrac{\dfrac{\varphi_0 \vdash \varphi'_0}{\varphi_0 \vdash \varphi'_0 + \varphi'_1}\,\mathtt{R}+_0 \qquad \dfrac{\varphi_1 \vdash \varphi'_1}{\varphi_1 \vdash \varphi'_0 + \varphi'_1}\,\mathtt{R}+_1}{v : \varphi_0 + \varphi_1 \vdash \varphi'_0 + \varphi'_1}\,\mathtt{L}+ \quad .$$

Le résultat recherché s'obtient alors simplement par induction sur $\mathcal{S}$. □

Par exemple, la Figure 4.3 présente la preuve Γ correspondant au système dirigé

$$\mathcal{S} = \left\{ \begin{array}{c} L =_3 1 + X \\ X =_1 N \times L \\ N =_1 1 + N \end{array} \right\}$$

des suites finies de nombres naturels. On a artificiellement placé la priorité de la variable L au-dessus des autres pour que Γ soit bien défini, mais comme cela ne change pas la sémantique du système, l'hypothèse $\mathsf{MAX}(\mathcal{S}) = \{X\}$ peut se faire sans perte de généralité.

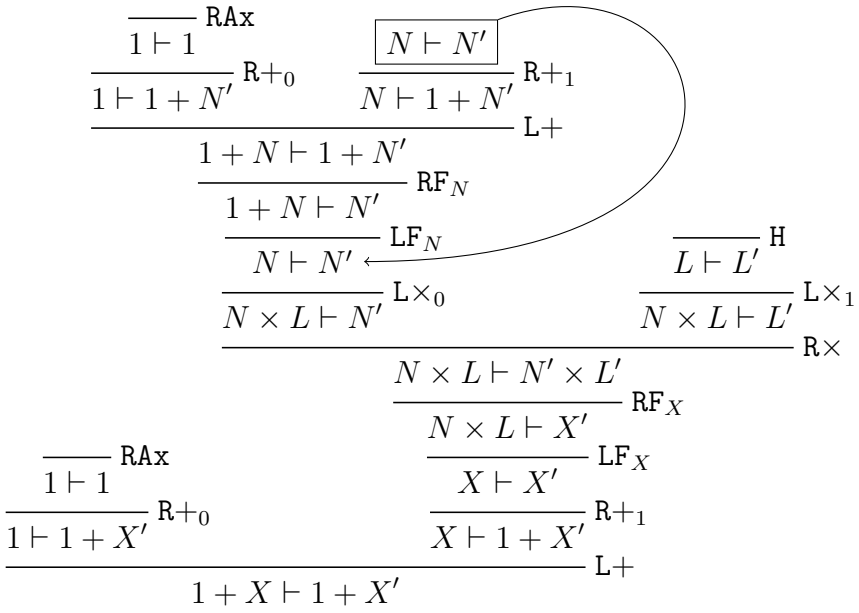


Figure 4.3 Une preuve par imitation

Rappelons que $\mathcal{M}$ dénote la catégorie μ-bicomplète libre (revoir la Section 2.6).

Théorème 4.7 (Plénitude)**.** *Pour toute flèche f de $\mathcal{M}$, il existe une preuve circulaire Π_f et un sommet $u \in \Pi_f$ tels que $[\![u]\!]_{\Pi_f} = f$.*

Démonstration. On procède par récurrence sur les constructeurs des flèches de la catégorie μ-bicomplète libre. Soit $s \xrightarrow{f} t$ une flèche de $\mathcal{M}$. Par la Proposition 2.12,

il existe deux formules, A et B, ainsi qu'un système dirigé d'équations, $\mathcal{S} = \mathcal{S}_s \cup \mathcal{S}_t$, tels que $\|s\|_V = [\![A]\!]_V^{\mathcal{S}}$ et $\|t\|_V = [\![B]\!]_V^{\mathcal{S}}$.

– Si $f \in \{\mathtt{id}, ?_t, !_s\}$, alors Π_f est la preuve de $A \vdash B$ à un seul sommet, justifié par `I`, `LAx` ou `RAx` respectivement.

– Si $t = (t_0 + t_1)$ et $f = \mathtt{in}_j$, alors $B = B_0 + B_1$ et on pose

$$\Pi_f := \dfrac{\dfrac{}{B_j \vdash B_j}\,\mathtt{I}}{B_j \vdash B_0 + B_1}\,\mathtt{R}{+_j}\ .$$

– Si $s = (s_0 \times s_1)$ et $f = \mathtt{pr}_j$, alors $A = A_0 \times A_1$ et on pose

$$\Pi_f := \dfrac{\dfrac{}{A_j \vdash A_j}\,\mathtt{I}}{A_0 \times A_1 \vdash A_j}\,\mathtt{L}{\times_j}\ .$$

– Si $t = \mu X.t'$ et $f = \alpha_t$, alors $\|t\| = [\![X]\!]$, $\|t'\| = [\![F_X]\!]$ et on pose

$$\Pi_f := \dfrac{\dfrac{}{F_X \vdash F_X}\,\mathtt{I}}{F_X \vdash X}\,\mathtt{RF}_X\ .$$

– Si $s = \nu X.s'$ et $f = \zeta_s$, alors $\|s\| = [\![X]\!]$, $\|s'\| = [\![F_X]\!]$ et on pose

$$\Pi_f := \dfrac{\dfrac{}{F_X \vdash F_X}\,\mathtt{I}}{X \vdash F_X}\,\mathtt{LF}_X\ .$$

– Si $f = h \cdot k$, alors par récurrence, Π_h et Π_k sont définies et on pose

$$\Pi_f := \dfrac{\dfrac{}{A \vdash C}\,\Pi_h \qquad \dfrac{}{C \vdash B}\,\Pi_k}{A \vdash B}\,\mathtt{C}\quad .$$

– Si $f = \langle h, k\rangle$, alors par récurrence, Π_h et Π_k sont définies et on pose

$$\Pi_f := \dfrac{\dfrac{}{A \vdash B_0}\,\Pi_h \qquad \dfrac{}{A \vdash B_1}\,\Pi_k}{A \vdash B_0 \times B_1}\,\mathtt{R}{\times}\ .$$

– Si $f = \{h, k\}$, alors par récurrence, Π_h et Π_k sont définies et on pose

$$\Pi_f := \dfrac{\dfrac{}{A_0 \vdash B}\,\Pi_h \qquad \dfrac{}{A_1 \vdash B}\,\Pi_k}{A_0 + A_1 \vdash B}\,\mathtt{L}{+}\ .$$

– Si $s = \mu X.s'$ et $f = a^s_g$ pour une certaine flèche $s'[X/t] \xrightarrow{g} t$, alors le diagramme suivant est commutatif.

$$\begin{array}{ccc} s'[X/s] & \xrightarrow{s'[X/f]} & s'[X/t] \\ {\scriptstyle \alpha_s}\downarrow & & \downarrow{\scriptstyle g} \\ s & \xrightarrow[f]{} & t \end{array}$$

Soit $\mathcal{S}_{s'} \subseteq \mathcal{S}$ comme dans la Proposition 2.12. Par la démonstration de celle-ci, on a $\|s'\|_V = [\![X]\!]^{\mathcal{T}}_V$ et on peut supposer, sans perte de généralité, que $\mathsf{MAX}(\mathcal{T}) = \{X\}$ (quitte à remplacer « $n \geq p_{\mathsf{MAX}(\mathcal{S}_{t'})}$ » par « $n > p_{\mathsf{MAX}(\mathcal{S}_{t'})}$ » dans la démonstration, ce qui ne change pas la sémantique du système). Remarquons également que puisque s est un μ-terme clos, alors la seule variable libre de s' est X et donc, la seule variable libre de $\mathcal{S}_{s'}$ est également X. Soit $H = [\![F_X]\!]^{\mathsf{P}(\mathcal{S}_{s'})}$.

Par l'hypothèse de récurrence, il existe une preuve circulaire Π_g sur $\mathcal{S}$ avec un sommet $v \in \Pi_g$ tel que $[\![v]\!]^{\mathcal{S}}_{\Pi_g} = g$. Soit $\textsc{Seq}(v) = A \vdash B$. Puisqu'on doit avoir $[\![A]\!]^{\mathcal{S}} = \|s'[X/t]\|$ et $[\![B]\!]^{\mathcal{S}} = \|t\|$, alors pour pouvoir exprimer ces foncteurs par des formules, il doit y avoir un sous-système $\mathcal{T} \subseteq \mathcal{S}$ qui est une copie de $\mathcal{S}_{s'}$, mais dans laquelle chaque instance de X est remplacée par B. On a donc

$$\begin{aligned} [\![A]\!]^{\mathcal{S}} &= \|s'[X/t]\| \\ &= \|s'\| \circ \|t\| \\ &= [\![F_X]\!]^{\mathsf{P}(\mathcal{T})}([\![B]\!]^{\mathcal{S}}) \\ &= [\![F_X]\!]^{\mathsf{P}(\mathcal{S}_{s'})}([\![B]\!]^{\mathcal{S}}) \\ &= H([\![B]\!]^{\mathcal{S}})\,. \end{aligned}$$

On a donc que $g : H([\![B]\!]^{\mathcal{S}}) \to [\![B]\!]^{\mathcal{S}}$ est une H-algèbre. Soit Γ comme dans le

Lemme 4.6. On pose alors :

$$\Pi_f := \quad \cfrac{\cfrac{\boxed{X \vdash B}}{\vdots\ \Gamma[X'/B]}\qquad \cfrac{}{F_X[X/B] \vdash B}\,\Pi_g}{\cfrac{F_X \vdash F_X[X/B]}{F_X \vdash B}\,\mathtt{C}}\,\mathtt{LF}_X \quad .$$

En effet, soit u la racine de cette preuve et $f = [\![u]\!]_{\Pi_{a_h^s}}$. Alors en se référant au Tableau 3.2, on obtient que f doit satisfaire :

$$\begin{aligned} f &= \alpha_X^{-1} \cdot [\![!\Gamma[X'/B]]\!](f) \cdot g \\ &= \alpha_X^{-1} \cdot [!\Gamma]_{c,[\![B]\!]c}(f) \cdot g \\ &= \alpha_X^{-1} \cdot H(f) \cdot g \\ &= \alpha_X^{-1} \cdot \|s'\|(f) \cdot g \\ &= \alpha_X^{-1} \cdot s'[X/f] \cdot g\,. \end{aligned}$$

– Si $t = \nu X.t'$ et $f = z_g^t$ pour une certaine flèche $s \xrightarrow{g} t'[X/s]$, alors le diagramme suivant doit être commutatif.

$$\begin{array}{ccc} s & \xrightarrow{\quad f \quad} & t \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle \zeta_t} \\ t'[X/s] & \xrightarrow[t'[X/f]]{} & t'[X/t] \end{array}$$

Par un raisonnement dual au cas précédent, on peut construire une preuve de la forme suivante :

$$\Pi_f := \quad \cfrac{\cfrac{}{A \vdash F_X[X/A]}\,\Pi_g \qquad \cfrac{\boxed{A \vdash X}}{\vdots\ \Gamma[X'/A]}}{\cfrac{A \vdash F_X}{A \vdash X}\,\mathtt{RF}_X}\,\mathtt{C} \quad ,$$

telle que si u est la racine de cette preuve et $f = [\![u]\!]_{\Pi_{z_f}}$, alors :

$$f = g \cdot t'[X/f] \cdot \zeta_X^{-1}\,. \qquad \square$$

CHAPITRE V

ÉLIMINATION DES COUPURES

Le *Hauptsatz*, ou théorème d'élimination des coupures de Gentzen (1935) † est en quelque sorte le théorème fondamental de la théorie des preuves. Il stipule que pour toute preuve Π dans les systèmes **LJ** et **LK** (formalisant respectivement la logique intuitionniste et la logique classique), il existe une autre preuve Π' de la même conclusion, mais qui n'utilise pas la règle de coupure. Comme premières applications de ce résultat, Gentzen démontre la décidabilité de la logique propositionnelle et la cohérence de l'arithmétique.

L'objectif de ce chapitre est de démontrer un théorème d'élimination des coupures pour les preuves circulaires. Le lecteur qui fut attentif à la Section 4.3 objectera sans doute, avec raison, qu'on a mentionné que le système déductif des preuves circulaires sans coupures de (Santocanale, 2001) n'était pas plein, en ce sens qu'il ne permettait pas, par exemple, d'exprimer la fonction diagonale $\Delta : \mathbb{N} \to \mathbb{N}^2$. Pourtant, on a donné une preuve *avec coupures* dénotant cette fonction à la Figure 4.2. Comment alors éliminer la coupure dans cette preuve ?

On décrit en fait un algorithme qui, étant donné une preuve circulaire close Π et un choix de conclusion dans celle-ci, construit bel et bien une preuve sans coupure

---

†. Voir (David *et al.*, 2004) pour une présentation complète et une preuve de ce théorème.

de la même conclusion, mais cette preuve est *possiblement infinie*. Comme dans le cas classique, l'algorithme d'élimination des coupures consistera en une stratégie, opérée par une sorte d'automate, pour éloigner les coupures de la racine de la preuve. Pour y parvenir, les mouvements recherchés consistent en des transpositions de la coupure avec l'un de ses successeurs du graphe de la preuve. Or, plutôt que d'*attirer* les coupures vers les axiomes, que les preuves circulaires n'ont pas nécessairement, on devra plutôt *repousser* les coupures vers l'infini. La limite de ce processus sera alors la preuve infinie recherchée.

Plutôt que de reposer sur un argument de complexité décroissante des formules comme pour le théorème de Gentzen, la preuve de la productivité de l'algorithme repose cette-fois sur la condition de garde. On démontre, par ailleurs, que la preuve infinie résultante satisfait encore la condition de garde (sur les chemins infinis).

Les éléments de ce chapitre sont purement syntaxiques, l'aspect sémantique des preuves infinies et son lien avec la sémantique des preuves circulaires étant plutôt repoussés au Chapitre 6. Les résultats principaux de ce chapitre sont publiés dans (Fortier et Santocanale, 2013).

5.1 Multicoupures

Il faudra composer avec un cas de transposition de règles qui ne se présente pas dans les travaux de Gentzen. Que faire lorsqu'une coupure est justifiée par une autre coupure ? Inutile de les transposer, puisque cela ne fait pas monter d'un cran le niveau où il y a une coupure (souvenons-nous de l'associativité) :

$$\dfrac{\dfrac{A \xrightarrow{f} C \quad C \xrightarrow{g} D}{A \xrightarrow{f\cdot g} D}\,\mathtt{C} \qquad D \xrightarrow{h} B}{A \xrightarrow{(f\cdot g)\cdot h} B}\,\mathtt{C} \quad = \quad \dfrac{A \xrightarrow{f} C \qquad \dfrac{C \xrightarrow{g} D \quad D \xrightarrow{h} B}{C \xrightarrow{g\cdot h} B}\,\mathtt{C}}{A \xrightarrow{f\cdot(g\cdot h)} B}\,\mathtt{C} \;.$$

On traite ce problème en *fusionnant* les coupures consécutives :

$$\frac{A \xrightarrow{f} B \quad B \xrightarrow{g} C \quad C \xrightarrow{h} D}{A \xrightarrow{f \cdot g \cdot h} D}\,\mathtt{C}\,.$$

On a donc besoin d'une structure de données qui s'apparente à une coupure d'arité quelconque.

Définition. Une ***multicoupure*** sur une pré-preuve Π est une liste finie et non vide $M := [u_1, \ldots, u_m]$ de sommets de Π telle que pour tout $i = 1 \ldots n-1$, les sommets u_i et u_{i+1} sont ***composables***, c'est-à-dire qu'ils satisfont l'équation $\textsc{Seq}_{\mathtt{R}}(u_i) = \textsc{Seq}_{\mathtt{L}}(u_{i+1})$. L'ensemble des multicoupures sur Π est dénoté $\mathcal{M}_\Pi$.

Étant donné une multicoupure $M = [u_1, \ldots, u_m]$, s'il s'avère qu'un des u_i est lui-même une coupure, on veut pouvoir le fusionner à M. On définit donc la fonction partielle suivante :

$$\textsc{Fusion} : \mathcal{M}_\Pi \times \mathbb{N} \rightharpoonup \mathcal{M}_\Pi$$
$$([u_0 \ldots, u_i, \ldots u_m], i) \mapsto [u_0 \ldots, \varsigma_0 u_i, \varsigma_1 u_i, \ldots u_m] \qquad (\text{si } \textsc{Seq}(u_i) = \mathtt{C}).$$

On peut illustrer cette opération schématiquement comme suit :

$$\frac{A_0 \vdash \ldots \vdash A_i \qquad \dfrac{A_i \vdash B \quad B \vdash A_{i+1}}{A_i \vdash A_{i+1}}\,\mathtt{C} \qquad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}$$

$$\Downarrow_{\textsc{Fusion}}$$

$$\frac{A_0 \vdash \ldots \vdash A_i \quad A_i \vdash B \quad B \vdash A_{i+1} \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}\,.$$

Une autre opération qu'on souhaite pouvoir opérer sur les multicoupures est l'élimination des identités qu'elles contiennent, puisque celles-ci ne contribuent pas à

la composition de fonctions que représente la coupure. On pose donc :

$$\begin{aligned}&\textsc{IdÉlim} : \mathcal{M}_\Pi \times \mathbb{N} \rightharpoonup \mathcal{M}_\Pi\\ &\qquad([\ldots u_{i-1}, u_i, u_{i+1}\ldots], i) \mapsto [\ldots u_{i-1}, u_{i+1}\ldots] \quad (\text{si } m > 1 \text{ et } \textsc{Seq}(u_i) = \mathtt{I}).\end{aligned}$$

On peut représenter cette opération comme suit :

$$\dfrac{A_0 \vdash \ldots \vdash B \qquad \dfrac{}{B \vdash B}\,\mathtt{I} \qquad B \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C} \quad \overset{\textsc{IdÉlim}}{\Longrightarrow} \quad \dfrac{A_0 \vdash \ldots \vdash B \qquad B \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}\,.$$

La prochaine opération est plus subtile. Supposons que dans une multicoupure $M = [u_0 \ldots u_m]$, on ait $\textsc{Règ}(u_i) \in \mathfrak{R}$ et $\textsc{Règ}(u_{i+1}) \in \mathfrak{L}$ pour un certain i. Notons que cela signifie $A_i := \textsc{Seq}_{\mathtt{R}}(u_i) = \textsc{Seq}_{\mathtt{L}}(u_{i+1})$ et que cette formule commune peut être soit un produit ou un coproduit de formules, une variable liée, ou une constante parmi 0 et 1. On peut supprimer tout de suite la possibilité d'une constante car $\textsc{Règ}(u_i) \in \mathfrak{R}$ impliquerait $A_i \neq 0$ et $\textsc{Règ}(u_{i+1}) \in \mathfrak{L}$ impliquerait $A_i \neq 1$, ce qui serait contradictoire. Il y a donc, en fait, trois scénarios possibles pour les valeurs de $\textsc{Règ}(u_i)$ et $\textsc{Règ}(u_{i+1})$: elles sont soit respectivement $\mathtt{R}\times$ et $\mathtt{L}\times_j$ pour un certain $j \in \{0, 1\}$, soit $\mathtt{R}+_j$ et $\mathtt{L}+$ pour un certain j, ou alors $\mathtt{RF}_X$ et $\mathtt{LF}_X$ pour une variable $X \in \mathsf{BV}(\mathcal{S})$. Dans chaque cas, on peut trouver des successeurs composables de u_i et u_{i+1} respectivement. On se donne alors une opération pour *réduire* u_i et u_{i+1} ensemble et les remplacer par leurs successeurs appropriés.

$$\begin{aligned}&\textsc{Réduct} : \mathcal{M}_\Pi \times \mathbb{N} \rightharpoonup \mathcal{M}_\Pi\\ &\qquad([\ldots u_i, u_{i+1}\ldots], i) \mapsto [\ldots \varsigma_p u_i, \varsigma_q u_{i+1}\ldots]\\ &\qquad\qquad(\text{si } \textsc{Règ}(u_i) \in \mathfrak{R} \text{ et } \textsc{Règ}(u_{i+1}) \in \mathfrak{L}),\end{aligned}$$

où p et q sont déterminés comme suit :

– si $\text{RÈG}(u_i) = \mathtt{R}\times$, $\text{RÈG}(u_{i+1}) = \mathtt{L}\times_j$ et $j \in \{0,1\}$, alors $p = j$ et $q = 0$:

$$\dfrac{A_0 \vdash \ldots \vdash A_{i-1} \quad \dfrac{A_{i-1} \vdash B_0 \quad A_{i-1} \vdash B_1}{A_{i-1} \vdash B_0 \times B_1}\,\mathtt{R}\times \quad \dfrac{B_j \vdash A_{i+1}}{B_0 \times B_1 \vdash A_{i+1}}\,\mathtt{L}\times_j \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}$$

$$\Downarrow_{\text{RÉDUCT}}$$

$$\dfrac{A_0 \vdash \ldots \vdash A_{i-1} \quad A_{i-1} \vdash B_j \quad B_j \vdash A_{i+1} \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}\,;$$

– si $\text{RÈG}(u_i) = \mathtt{R}+_j$, $\text{RÈG}(u_{i+1}) = \mathtt{L}+$ et $j \in \{0,1\}$, alors $p = 0$ et $q = j$:

$$\dfrac{A_0 \vdash \ldots \vdash A_{i-1} \quad \dfrac{A_{i-1} \vdash B_j}{A_{i-1} \vdash B_0 + B_1}\,\mathtt{R}+_j \quad \dfrac{B_0 \vdash A_{i+1} \quad B_1 \vdash A_{i+1}}{B_0 + B_1 \vdash A_{i+1}}\,\mathtt{L}+ \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}$$

$$\Downarrow_{\text{RÉDUCT}}$$

$$\dfrac{A_0 \vdash \ldots \vdash A_{i-1} \quad A_{i-1} \vdash B_j \quad B_j \vdash A_{i+1} \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}\,;$$

– si $\text{RÈG}(u_i) = \mathtt{RF}_X$, $\text{RÈG}(u_{i+1}) = \mathtt{LF}_X$ et $X \in \mathsf{BV}(\mathcal{S})$, alors $p = q = 0$:

$$\dfrac{A_0 \vdash \ldots \vdash A_{i-1} \quad \dfrac{A_{i-1} \vdash F_X}{A_{i-1} \vdash X}\,\mathtt{RF}_X \quad \dfrac{F_X \vdash A_{i+1}}{X \vdash A_{i+1}}\,\mathtt{LF}_X \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}$$

$$\Downarrow_{\text{RÉDUCT}}$$

$$\dfrac{A_0 \vdash \ldots \vdash A_{i-1} \quad A_{i-1} \vdash F_X \quad F_X \vdash A_{i+1} \quad A_{i+1} \vdash \ldots \vdash A_m}{A_0 \vdash A_m}\,\mathtt{C}\,.$$

Définition. Soit $M, N \in \mathcal{M}_\Pi$. S'il existe $\Phi \in \{\text{FUSION}, \text{IDÉLIM}, \text{RÉDUCT}\}$ et $i \in \mathbb{N}$ tels que $N = \Phi(M, i)$, alors on écrit $M \rightarrowtail N$. On définit aussi $\overset{*}{\rightarrowtail}$ comme étant la plus petite relation réflexive et transitive sur $\mathcal{M}_\Pi$ à contenir $\rightarrowtail$.

On a ainsi défini un préordre $\overset{*}{\rightarrowtail}$ sur $\mathcal{M}_\Pi$. La question naturelle qu'on est en droit de se poser est la suivante : s'agit-il d'une relation d'ordre ? La réponse

est affirmative, dans le cas où Π satisfait la condition de garde. Cela est une conséquence du théorème suivant, crucial pour l'élimination des coupures, dont on repousse la démonstration aux Sections 5.3 à 5.5.

Théorème 5.1. *Si Π satisfait la condition de garde, alors il n'existe aucune $\bowtie$-chaîne infinie dans $\mathcal{M}_\Pi$.*

Corollaire 5.2. *Si Π satisfait la condition de garde, alors la relation $\overset{*}{\bowtie}$ est un ordre partiel sur $\mathcal{M}_\Pi$.*

Démonstration. La relation $\overset{*}{\bowtie}$ est réflexive et transitive par définition. Il ne reste alors qu'à démontrer la propriété d'antisymétrie. Soit donc $M, N \in \mathcal{M}_\Pi$ tels que $M \overset{*}{\bowtie} N$ et $N \overset{*}{\bowtie} M$. Si $M \neq N$, alors il existe deux $\bowtie$-chaînes non triviales :

$$M = M_0 \bowtie M_1 \bowtie \ldots \bowtie M_k = N \quad \text{et} \quad N = N_0 \bowtie N_1 \bowtie \ldots \bowtie N_\ell = M \ .$$

En mettant ces deux chaînes bout-à-bout, on trouve un cycle dans $\mathcal{M}_\Pi$ et donc une $\bowtie$-chaîne infinie : une contradiction avec le Théorème 5.1. □

Enfin, mentionnons que, puisque les multicoupures sont, avant tout, des listes, on peut calculer leur concaténation, mais seulement dans le cas où elles sont composables. Ainsi, si $M = [u_1 \ldots u_m]$ et $N = [v_1 \ldots v_n]$ sont tels que $\textsc{Seq}_{\mathtt{R}}(u_m) = \textsc{Seq}_{\mathtt{L}}(v_1)$, soit :

$$M \cdot N := [u_1 \ldots u_m, v_1 \ldots v_n].$$

Le prochain Lemme dit que la concaténation est compatible avec la relation $\bowtie$ et, donc, aussi avec $\overset{*}{\bowtie}$.

Lemme 5.3. *Soit $M, N, U \in \mathcal{M}_\Pi$ tels que $M \bowtie N$. Alors $M \cdot U \bowtie N \cdot U$ et $U \cdot M \bowtie U \cdot N$, pourvu que ces expressions soient bien définies.*

Démonstration. Soit $\Phi \in \{\textsc{Fusion}, \textsc{IdÉlim}, \textsc{Réduct}\}$ et $i \in \mathbb{N}$ tels qu'on ait $N = \Phi(M, i)$. Si $M \cdot U$ et $N \cdot U$ sont bien définis, on vérifie aisément

$$N \cdot U = \Phi(M, i) \cdot U = \Phi(M \cdot U, i) \ .$$

Donc $M \cdot U \bowtie N \cdot U$. De la même manière, si $U \cdot M$ et $U \cdot N$ sont bien définis, on a

$$U \cdot N = U \cdot \Phi(M, i) = \Phi(U \cdot M, k + i)$$

où $k = |U|$. Donc $U \cdot M \bowtie U \cdot N$. □

5.2 Algorithme d'élimination des coupures

Tel que mentionné en introduction de ce chapitre, l'élimination des coupures dans une preuve Π se fait de façon analogue à la méthode de Gentzen, en permutant les coupures (ou dans notre cas, les multicoupures) avec un successeur bien choisi de celles-ci, pour ainsi les faire monter plus haut dans un arbre de preuve.

Définition. Une multicoupure $M = [u_1 \dots u_m]$ est ***productive à gauche*** si $\textsc{Règ}(u_1) \in \mathfrak{L}$ et ***productive à droite*** si $\textsc{Règ}(u_m) \in \mathfrak{R}$. L'ensemble des multicoupures productives à gauche est dénoté $\mathcal{M}_\Pi^{\mathtt{L}}$ et l'ensemble de celles qui sont productives à droite est dénoté $\mathcal{M}_\Pi^{\mathtt{R}}$.

Il reste à définir ce que ces multicoupures *produisent* (à gauche ou à droite). Essentiellement, une multicoupure productive M permet directement de construire un morceau d'un arbre infini sans coupure associé à celle-ci, dénoté $\textsc{ce}_\Pi(M)$, puis d'indiquer au programme qui construit cet arbre quelles sont les nouvelles multicoupures à traiter, via les deux fonctions

$$\textsc{LNext} : \mathcal{M}_\Pi^{\mathtt{L}} \to \mathcal{M}_\Pi^* \quad \text{et} \quad \textsc{RNext} : \mathcal{M}_\Pi^{\mathtt{R}} \to \mathcal{M}_\Pi^*$$

définies ci-dessous (où $\mathcal{M}_\Pi^*$ dénote, comme d'habitude, l'ensemble des listes finies de multicoupures). Les schémas présentés sous ces définitions servent à justifier celles-ci et à donner une intuition sur la façon dont on se servira des multicoupures productives dans la construction de la preuve sans coupures.

Commençons par le côté gauche. La fonction LNEXT est définie comme suit :

– si $\text{RÈG}(u_1) = \mathtt{LAx}$, alors $\text{LNEXT}(M) = [\,]$:

$$\dfrac{\dfrac{}{0 \vdash A_1}\,\mathtt{LAx} \qquad A_1 \vdash \ldots \vdash A_m}{0 \vdash A_m}\,\mathtt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{}{0 \vdash A_m}\,\mathtt{LAx}\ ;$$

– si $\text{RÈG}(u_1) = \mathtt{L}\times_j$, $j \in \{0,1\}$, alors $\text{LNEXT}(M) = \big[[\varsigma u_1, u_2 \ldots u_m]\big]$:

$$\dfrac{\dfrac{B_j \vdash A_1}{B_0 \times B_1 \vdash A_1}\,\mathtt{L}\times_j \qquad A_1 \vdash \ldots \vdash A_m}{B_0 \times B_1 \vdash A_m}\,\mathtt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{\dfrac{B_j \vdash A_1 \quad A_1 \vdash \ldots \vdash A_m}{B_j \vdash A_m}\,\mathtt{C}}{B_0 \times B_1 \vdash A_m}\,\mathtt{L}\times_j\ ;$$

– si $\text{RÈG}(u_1) = \mathtt{L}+$, alors $\text{LNEXT}(M) = \big[[\varsigma_0 u_1, u_2 \ldots u_m], [\varsigma_1 u_1, u_2 \ldots u_m]\big]$:

$$\dfrac{\dfrac{B_0 \vdash A_1 \quad B_1 \vdash A_1}{B_0 + B_1 \vdash A_1}\,\mathtt{L}+ \qquad A_1 \vdash \ldots \vdash A_m}{B_0 + B_1 \vdash A_m}\,\mathtt{C}$$

$$\Downarrow_{\text{LNEXT}}$$

$$\dfrac{\dfrac{B_0 \vdash A_1 \quad A_1 \vdash \ldots \vdash A_m}{B_0 \vdash A_m}\,\mathtt{C} \qquad \dfrac{B_1 \vdash A_1 \quad A_1 \vdash \ldots \vdash A_m}{B_1 \vdash A_m}\,\mathtt{C}}{B_0 + B_1 \vdash A_m}\,\mathtt{L}+\ ;$$

– si $\text{RÈG}(u_1) = \mathtt{LF}_X$, $X \in \mathsf{BV}(\mathcal{S})$, alors $\text{LNEXT}(M) = \big[[\varsigma u_1, u_2 \ldots u_m]\big]$:

$$\dfrac{\dfrac{F_X \vdash A_1}{X \vdash A_1}\,\mathtt{LF}_X \qquad A_1 \vdash \ldots \vdash A_m}{X \vdash A_m}\,\mathtt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{\dfrac{F_X \vdash A_1 \quad A_1 \vdash \ldots \vdash A_m}{F_X \vdash A_m}\,\mathtt{C}}{X \vdash A_m}\,\mathtt{LF}_X\ .$$

De façon duale, la fonction RNEXT est définie comme suit :

– si $\text{RÈG}(u_m) = \mathtt{RAx}$, alors $\text{RNEXT}(M) = [\,]$:

$$\frac{A_0 \vdash \ldots \vdash A_{m-1} \qquad \dfrac{}{A_{m-1} \vdash 1}\,\mathtt{RAx}}{A_0 \vdash 1}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \frac{}{A_0 \vdash 1}\,\mathtt{RAx}\,;$$

– si $\text{RÈG}(u_m) = \mathtt{R}\times$, alors $\text{RNEXT}(M) = \big[[u_1 \ldots u_{m-1}, \varsigma_0 u_m], [u_1 \ldots u_{m-1}, \varsigma_1 u_m]\big]$:

$$\frac{A_0 \vdash \ldots \vdash A_{m-1} \qquad \dfrac{A_{m-1} \vdash B_0 \quad A_{m-1} \vdash B_1}{A_{m-1} \vdash B_0 \times B_1}\,\mathtt{R}\times}{A_0 \vdash B_0 \times B_1}\,\mathtt{C}$$

$$\Downarrow_{\text{RNEXT}}$$

$$\frac{\dfrac{A_0 \vdash \ldots \vdash A_{m-1} \quad A_{m-1} \vdash B_0}{A_0 \vdash B_1}\,\mathtt{C} \qquad \dfrac{A_0 \vdash \ldots \vdash A_{m-1} \quad A_{m-1} \vdash B_1}{A_0 \vdash B_1}\,\mathtt{C}}{A_0 \vdash B_0 \times B_1}\,\mathtt{R}\times\,;$$

– si $\text{RÈG}(u_m) = \mathtt{R}+_j$, $j \in \{0,1\}$, alors $\text{RNEXT}(M) = \big[[u_1 \ldots u_{m-1}, \varsigma u_m]\big]$:

$$\frac{A_0 \vdash \ldots \vdash A_{m-1} \qquad \dfrac{A_{m-1} \vdash B_j}{A_{m-1} \vdash B_0 + B_1}\,\mathtt{R}+_j}{A_0 \vdash B_0 + B_1}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \frac{\dfrac{A_0 \vdash \ldots \vdash A_{m-1} \quad A_{m-1} \vdash B_j}{A_0 \vdash B_j}\,\mathtt{C}}{A_0 \vdash B_0 + B_1}\,\mathtt{R}+_j\,;$$

– si $\text{RÈG}(u_m) = \mathtt{RF}_X$, $X \in \mathsf{BV}(\mathcal{S})$, alors $\text{RNEXT}(M) = \big[[u_1 \ldots u_{m-1}, \varsigma u_m]\big]$:

$$\frac{A_0 \vdash \ldots \vdash A_{m-1} \qquad \dfrac{A_{m-1} \vdash F_X}{A_{m-1} \vdash X}\,\mathtt{RF}_X}{A_0 \vdash X}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \frac{\dfrac{A_0 \vdash \ldots \vdash A_{m-1} \quad A_{m-1} \vdash F_X}{A_0 \vdash F_X}\,\mathtt{C}}{A_0 \vdash X}\,\mathtt{RF}_X\,.$$

Définition. Une pré-preuve de $\mathbf{C}_{\mathcal{S}}$ est dite ***arborescente*** si son support est un arbre (possiblement infini). La racine d'une telle pré-preuve sera indistinctement dénotée par le symbole ε.

Lemme 5.4. *Soit* Ψ *une pré-preuve arborescente sans coupures telle que* $\textsc{Seq}_{\mathtt{L}}(\varepsilon) = 1$. *Alors pour tout* $u \in \Psi$, $\textsc{Règ}(u) \in \mathfrak{R} \cup \{\mathtt{I}\}$ *et* $\textsc{Seq}_{\mathtt{L}}(u) = 1$.

Démonstration. Par inspection du Tableau 3.1, aucune règle gauche ne peut justifier un séquent de la forme $1 \vdash \varphi$. Une simple induction sur u suffit alors à démontrer le résultat. □

On arrive au point de définir la pré-preuve arborescente sans coupures correspondant à $M \in \mathcal{M}_\Pi$. Comme il s'agit d'un objet possiblement infini, on privilégiera une définition *paresseuse* de cette pré-preuve, qui pourrait être implémentée dans un langage de programmation fonctionnelle. † Notons qu'une pré-preuve arborescente est simplement un arbre, possiblement infini, à branchements finis doublement étiquetés (par des séquents et par des règles), avec la contrainte supplémentaire de satisfaire l'arité des règles. Ce sont donc des éléments de $\mathcal{T}_{\Sigma\times\mathsf{SEQ}_\mathfrak{F}}$ (revoir l'Exemple 5 de la Section 2.3). Rappelons que cet ensemble est muni d'un constructeur de type :

$$\begin{aligned} \mathtt{Cons} \ : \ (\Sigma \times \mathsf{SEQ}_\mathfrak{F}) \times \mathcal{T}^*_{\Sigma\times\mathsf{SEQ}_\mathfrak{F}} &\to \mathcal{T}_{\Sigma\times\mathsf{SEQ}_\mathfrak{F}} \,, \\ (\langle \rho, \sigma\rangle, [t_1 \dots t_n]) \ &\mapsto \ \frac{t_1 \ \dots \ t_n}{\sigma}\, \rho \,. \end{aligned}$$

Lemme 5.5. *Soit* Π *une pré-preuve close* $M \in \mathcal{M}_\Pi$. *Alors il y a quatre possibilités (pas nécessairement mutuellement exclusives) :* $M \in \mathcal{M}^{\mathtt{L}}_\Pi$, $M \in \mathcal{M}^{\mathtt{R}}_\Pi$, $M = [u]$ *avec* $\textsc{Règ}(u) = \mathtt{I}$ *et enfin,* $\exists N \in \mathcal{M}_\Pi$ *tel que* $M \bowtie N$.

Démonstration. Soit $M = [u_1 \dots u_m]$. S'il y a un certain i tel que $\textsc{Règ}(u_i) = \mathtt{I}$ alors soit c'est le seul élément de M (comme dans l'énoncé du lemme), soit on

---

†. Notons qu'on pourrait aussi définir $\textsc{ce}_\Pi(M)$ par un algorithme impératif utilisant une boucle infinie comme on a fait dans (Fortier et Santocanale, 2013), mais ce serait moins élégant et moins dans l'esprit de cette thèse.

peut prendre $N = \textsc{IdÉlim}(M, i)$. Supposons donc qu'aucun des u_i n'est justifié par la règle $\mathtt{I}$. S'il existe i tel que $\textsc{Règ}(u_i) = \mathtt{C}$, alors similairement, on peut prendre $N = \textsc{Fusion}(M, i)$. Sinon, puisque Π est close, on sait que pour tout i, $\textsc{Règ}(u_i) \in \mathfrak{L} \cup \mathfrak{R}$.

Supposons donc qu'on se trouve dans une telle situation et que, de plus, on ait $M \notin \mathcal{M}_\Pi^{\mathtt{L}} \cup \mathcal{M}_\Pi^{\mathtt{R}}$. C'est-à-dire $\textsc{Règ}(u_1) \in \mathfrak{R}$ et $\textsc{Règ}(u_m) \in \mathfrak{L}$. Soit L l'ensemble des indices i pour lesquels $\textsc{Règ}(u_i) \in \mathfrak{L}$. Puisque $u_m \in L$, alors $L \neq \varnothing$ et on peut donc poser $\ell = \min(L)$. On a donc $\textsc{Règ}(u_\ell) \in \mathfrak{L}$ et, puisque $\textsc{Règ}(u_1) \in \mathfrak{R}$, on a $\ell > 1$. Par minimalité, on a donc $\textsc{Règ}(u_{\ell-1}) \in \mathfrak{R}$ et il suffit de prendre $N = \textsc{Réduct}(M, \ell - 1)$. □

Définition. Soit $M = [u_1 \dots u_m] \in \mathcal{M}_\Pi$. Alors la ***pré-preuve sans coupures associée à*** M, dénotée $\textsc{ce}_\Pi(M)$, est définie comme suit :

1. si $m = 1$, $\textsc{Seq}(u_1) = A \vdash A$ et $\textsc{Règ}(u_1) = \mathtt{I}$, alors $\textsc{ce}_\Pi(M) := \dfrac{}{A \vdash A}\,\mathtt{I}$;
2. s'il existe $N \in \mathcal{M}_\Pi$ tel que $M \bowtie N$, alors $\textsc{ce}_\Pi(M) := \textsc{ce}_\Pi(N)$;
3. si $M \in \mathcal{M}_\Pi^{\mathtt{L}}$, alors $\textsc{ce}_\Pi(M) := \mathtt{Cons}(\langle \rho, \sigma \rangle, L)$ où
$$\begin{aligned} \rho &= \textsc{Règ}(u_1)\,, \\ \sigma &= \textsc{Seq}_{\mathtt{L}}(u_1) \vdash \textsc{Seq}_{\mathtt{R}}(u_m)\,, \\ L &= \mathtt{map}_{\textsc{ce}_\Pi}(\textsc{LNext}(M))\,; \end{aligned}$$
4. si $M \in \mathcal{M}_\Pi^{\mathtt{R}}$, alors $\textsc{ce}_\Pi(M) := \mathtt{Cons}(\langle \rho, \sigma \rangle, L)$ où
$$\begin{aligned} \rho &= \textsc{Règ}(u_m)\,, \\ \sigma &= \textsc{Seq}_{\mathtt{L}}(u_1) \vdash \textsc{Seq}_{\mathtt{R}}(u_m)\,, \\ L &= \mathtt{map}_{\textsc{ce}_\Pi}(\textsc{RNext}(M))\,. \end{aligned}$$

Creusons-nous un peu les méninges pour nous assurer que la définition ci-dessus est une *bonne* définition. Le cas 1 ne cause évidemment aucun problème car il ne

fait pas récursivement appel à la fonction CE_Π qu'on est en train de définir. Les cas 3 et 4 font un tel appel récursif, mais celui-ci est *gardé*, au sens de (Coquand, 1993), par le constructeur `Cons`, ce qui en garantit la productivité. C'est-à-dire que la fonction CE_Π ne fait pas, dans ces deux cas, un appel à elle-même sans construire un morceau d'arbre au passage. Quant au cas 2, il fait bel et bien un appel non gardé à lui-même et pourrait donc être problématique si l'on venait à le réitérer une infinité de fois sans faire appel aux cas 1, 3 et 4. Or, cela ne peut pas se produire grâce au Théorème 5.1, qu'il nous reste encore à démontrer.

Au passage, les outils qu'on développera pour faire cette démonstration nous permettront d'affirmer que $\text{CE}_\Pi(M)$ est non seulement une pré-preuve arborescente, mais qu'il s'agit même d'une *preuve* arborescente.

Théorème 5.6. *Si* Π *satisfait la condition de garde, alors pour tout* $M \in \mathcal{M}_\Pi$*, la pré-preuve* $\text{CE}_\Pi(M)$ *satisfait elle-même la condition de garde* **G2** *sur les chemins infinis.*

5.3 Trace complète d'une exécution

Soit $M \in \mathcal{M}_\Pi$. L'algorithme obtenu en déroulant (indéfiniment) la définition de $\text{CE}_\Pi(M)$ peut être vu comme étant l'ouvrage d'une sorte d'automate d'arbre avec mémoire. Les états possibles de la mémoire sont les multicoupures et les opérations Fusion, IdÉlim et Réduct sont des transitions muettes qui modifient cette mémoire. Quant aux productions, on peut les imaginer comme un choix non déterministe, de la part de l'automate, d'une branche de $\text{CE}_\Pi(M)$ qu'il tente de construire. Selon son choix, il écrira un morceau d'arbre et modifiera la mémoire pour se trouver dans un nouvel état $M' \in \text{LNext}(M)$ ou $M' \in \text{RNext}(M)$, selon le cas. On explorera plus en détails l'analogie entre automates avec mémoire et élimination des coupures au Chapitre 7, mais il est bon de garder en tête que

toutes les opérations définies sur les multicoupures donnent à $\mathcal{M}_\Pi$ la structure d'une sorte de graphe des configurations d'un automate.

Lors d'une exécution infinie de cet automate, ce dernier passera par une suite infinie $(M_n)_{n\in\mathbb{N}}$ de multicoupures telle que $M = M_0$ et, pour tout n, ou bien $M_n \bowtie M_{n+1}$, ou bien $M_{n+1} \in \textsc{LNext}(M_n)$, ou encore, $M_{n+1} \in \textsc{RNext}(M_n)$. On souhaite garder une trace de chacune des modifications locales qui surviennent dans la mémoire lors de ces transitions. La ***trace complète*** de l'exécution, dénotée T, est ainsi définie comme étant le plus petit graphe étiqueté par $\mathbb{N}$ dont le support est un sous-ensemble de $(\mathbb{N}\times\mathbb{N})\cup\{*\}$, contenant le point $*$ et dont les transitions sont les suivantes :

– pour $1 \le i \le |M_0|$,

$$* \xrightarrow{i} (0, i)\ ;$$

– si $M_{n+1} = \textsc{IdÉlim}(M_n, i)$, alors

$$\begin{aligned} (n,k) &\xrightarrow{0} (n+1,k) && \text{pour } k < i,\\ (n,k) &\xrightarrow{0} (n+1,k-1) && \text{pour } k > i\,; \end{aligned}$$

– si $M_{n+1} = \textsc{Fusion}(M_n, i)$, alors

$$\begin{aligned} (n,k) &\xrightarrow{0} (n+1,k) && \text{pour } k < i,\\ (n,k) &\xrightarrow{0} (n+1,k+1) && \text{pour } k > i,\\ (n,i) &\xrightarrow{1} (n+1,i)\ ,\\ (n,i) &\xrightarrow{2} (n+1,i+1)\ ; \end{aligned}$$

– si $M_{n+1} = \textsc{Réduct}(M_n, i)$, alors

$$\begin{aligned} (n,k) &\xrightarrow{3} (n+1,k) && \text{pour } k \in \{i, i+1\},\\ (n,k) &\xrightarrow{0} (n+1,k) && \text{pour les autres } k\,; \end{aligned}$$

– si $M_{n+1} \in \text{LNext}(M_n)$, alors

$$(n,k) \xrightarrow{0} (n+1,k) \qquad \text{pour } k > 1,$$
$$(n,1) \xrightarrow{4} (n+1,1)\ ;$$

– si $M_{n+1} \in \text{RNext}(M_n)$, alors

$$(n,k) \xrightarrow{0} (n+1,k) \qquad \text{pour } k < |M_n|,$$
$$(n,k) \xrightarrow{5} (n+1,k) \qquad \text{pour } k = |M_n|.$$

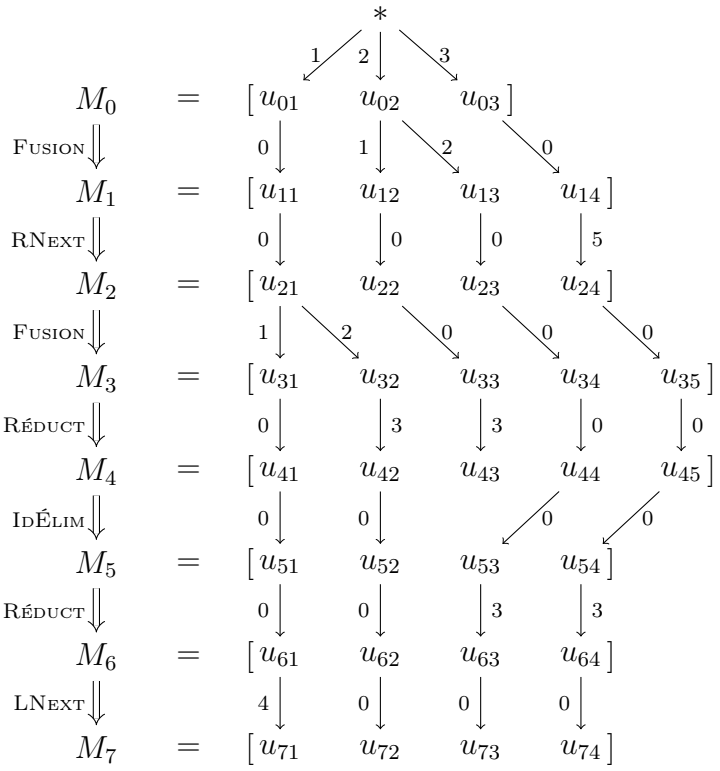


Figure 5.1 Début de la trace complète d'une exécution

La Figure 5.1 illustre de quoi pourrait avoir l'air la trace d'une exécution donnée. Puisque chaque transition dans le graphe T (sauf celles qui partent de $*$) est de la forme $(n,k) \to (n+1,k')$, alors aucun retour en-arrière n'est possible et on en conclut que T est un arbre infini dont la racine est $*$. De plus, par construction, T

est un graphe déterministe à branchements finis. Tel que convenu à la Section 1.4, on se permettra d'identifier les sommets de T, qui sont des coordonnées, aux mots qui mènent à ceux-ci depuis $*$. Cela nous permet de définir les relations d'ordre $\sqsubseteq$ et $\preceq$ de la Section 1.2 sur T.

Lemme 5.7. *Pour tout $n \in \mathbb{N}$ et $(n,k_1),(n,k_2) \in T$, $(n,k_1) \prec (n,k_2)$ si et seulement si $k_1 < k_2$.*

Démonstration. Par induction sur n. □

Dans l'espoir de démontrer les Théorèmes 5.1 et 5.6, il faudra garder un oeil aur les sommets de T sur lesquels un morceau de $\textsc{ce}_\Pi(M)$ est produit. On appellera simplement ces sommets ***producteurs*** et on les regroupe en deux familles :

$$P_{\mathtt{L}} = \left\{ u \in T \setminus \{*\} : \exists u' \text{ t.q. } u \xrightarrow{4} u' \right\};$$
$$P_{\mathtt{R}} = \left\{ u \in T \setminus \{*\} : \exists u' \text{ t.q. } u \xrightarrow{5} u' \right\}.$$

Notons que puisque M a été pris quelconque, alors le Théorème 5.1 sera démontré si et seulement si on parvient à démontrer que nécessairement, $P_{\mathtt{L}} \cup P_{\mathtt{R}} \neq \varnothing$.

Lemme 5.8. *Soit β une branche infinie de T. Alors pour tout $u \in P_{\mathtt{L}}$, ou bien $u \sqsubset \beta$, ou alors $u \prec \beta$. De façon similaire, pour tout $u \in P_{\mathtt{R}}$, ou bien $u \sqsubset \beta$, ou alors $u \succ \beta$.*

Démonstration. Soit $u \in P_{\mathtt{L}}$. Alors $u = (n,0)$ pour un certain n. Puisque β est une branche infinie, il existe un k tel que $v := (n,k) \sqsubset \beta$. Si $k = 0$, alors $u = v$ et donc $u \sqsubset \beta$. Sinon, $k > 0$ et par le Lemme 5.7, $u \prec v$. Ainsi donc, $u \prec \beta$.

De façon similaire, soit $u \in P_{\mathtt{R}}$. Alors $u = (n, |M_n|)$ pour un certain n. Puisque β est une branche infinie, il existe un k tel que $v := (n,k) \sqsubset \beta$. Si $k = |M_n|$, alors $u = v$ et donc $u \sqsubset \beta$. Sinon, $k < |M_n|$ et par le Lemme 5.7, $u \succ v$. Ainsi donc, $u \prec \beta$. □

Définition. Pour tout $u = (n, k) \in T \setminus \{*\}$, soit $g(u) \in \Pi$ le k-ième élément élément de M_n.

Lemme 5.9. *Soit $u \in T \setminus \{*\}$ et soit $v := u \cdot 0^k \in T$. Alors $g(u) = g(v)$.*

Démonstration. Par induction sur k, puisque les transitions étiquetées par 0 sont celles qui ne changent pas la valeur de la fonction g. □

Par abus de langage, on peut définir $\text{RÈG} : T \setminus \{*\} \to \Sigma$ par l'équation

$$\text{RÈG}(u) := \text{RÈG}(g(u)) \ . \tag{5.1}$$

Définition. Soit n et i tels que $M_{n+1} = \text{RÉDUCT}(M_n, i)$. Soit $u = (n, i)$ et $v = (n, i + 1)$. Alors u et v sont dits ***jumelés***, ou encore on dira qu'ils sont ***jumeaux*** l'un de l'autre et on écrira $\text{jum}(u) = v$ et $\text{jum}(v) = u$.

Il suit directement de cette définition que la fonction partielle jum est une involution (là où elle est définie), c'est-à-dire $\text{jum}(\text{jum}(u)) = u$ pour tout u. Aussi, le Lemme 5.7 entraîne qu'on a toujours soit $u \prec \text{jum}(u)$ ou bien $\text{jum}(u) \prec u$. Enfin, le Lemme suivant découle directement de la définition de RÉDUCT.

Lemme 5.10. *Soit $u_1, u_2 \in T$ des jumeaux. Alors $u_1 \prec u_2$ si et seulement si l'une des situations suivantes se produit :*

- $\text{RÈG}(u_1) = \mathtt{R}\times$ *et* $\text{RÈG}(u_2) = \mathtt{L}\times_j$ *où* $j \in \{0, 1\}$;
- $\text{RÈG}(u_1) = \mathtt{R}+_j$ *et* $\text{RÈG}(u_2) = \mathtt{L}+$ *où* $j \in \{0, 1\}$;
- $\text{RÈG}(u_1) = \mathtt{RF}_X$ *et* $\text{RÈG}(u_2) = \mathtt{LF}_X$ *où* $X \in \mathsf{BV}(S)$.

Lemme 5.11. *Soit β une branche infinie de T et soit $u \in T$ un sommet jumelé. Alors :*

1. *si $u \prec \beta$, alors soit* $\text{jum}(u) \prec \beta$ *ou bien* $\text{jum}(u) \sqsubset \beta$;
2. *si $u \succ \beta$, alors soit* $\text{jum}(u) \succ \beta$ *ou bien* $\text{jum}(u) \sqsubset \beta$.

Démonstration. On démontre seulement le cas 1, la démonstration du cas 2 lui étant parfaitement symétrique.

Supposons qu'on ait $u \prec \beta$. Si $\mathrm{jum}(u) \prec u$, le résultat découle de la transitivité de $\prec$. Supposons donc qu'on ait $\mathrm{jum}(u) \succ u$. Soit $n, i \in \mathbb{N}$ tels que $u = (n, i)$ et $\mathrm{jum}(u) = (n, i+1)$.

Puisque β est une branche infinie, il existe $v \sqsubset \beta$ tel que $|v| = n+1$. Cela signifie que $v = (n, k)$ pour un certain k. Si $k = i$, alors $v = u$ et donc $u \sqsubset \beta$, une contradiction avec $u \prec \beta$. Si $k < i$, alors par le Lemme 5.7, $v \prec u$ et donc $\beta \prec u$, encore une contradiction. La seule possibilité restante est donc $k > i$.

Dans ce cas, si $k = i + 1$, alors $v = \mathrm{jum}(u)$ et donc $\mathrm{jum}(u) \sqsubset \beta$ comme voulu. Sinon, $k > i+1$ et par le Lemme 5.7, $v \succ \mathrm{jum}(u)$. Il s'ensuit que $\beta \succ \mathrm{jum}(u)$. □

5.4 Trace effective d'une exécution

Comme on l'a remarqué au Lemme 5.9, les transitions étiquetées par 0 dans T ne représentent pas des transitions de la preuve originale Π et ne sont là que pour tracer l'historique des sommets qu'elles touchent. Afin d'exploiter le fait que Π satisfait la condition de garde – ce qui est l'hypothèse des Théorèmes 5.1 et 5.6 qu'on cherche, rappelons-le, à démontrer – on devra d'abord s'assurer que les chemins dans la trace correspondent à de véritables chemins dans Π. Cela implique de sacrifier les transitions étiquetées par 0. Soit donc $\psi : \mathbb{N}^* \to \mathbb{N}^*$ le morphisme engendré par les équations suivantes :

$$\psi(a) = a \quad (\forall a > 0) \qquad , \qquad \psi(0) = \varepsilon \ .$$

Lemme 5.12. *Soit $u, v \in T$. Alors $\psi(u) = \psi(v)$ si et seulement s'il existe $w \in T$ et $j, k \in \mathbb{N}$ tels que $u = w \cdot 0^j$ et $v = w \cdot 0^k$.*

Démonstration. Si $u = w \cdot 0^j$ et $v = w \cdot 0^k$, alors

$$\psi(u) = \psi(w \cdot 0^j) = \psi(w)\psi(0)^j = \psi(w) = \psi(w)\psi(0)^k = \psi(w \cdot 0^k) = \psi(v).$$

Réciproquement, supposons qu'on ait $\psi(u) = \psi(v)$. Si $u \prec v$ ou $v \prec u$, alors on peut écrire

$$u = wau' \quad \text{et} \quad v = wbv' \,,$$

où $w \in T$, $a, b \in \mathbb{N}$ et $a \neq b$. On remarque qu'on ne peut avoir $a = 0$ ou $b = 0$ puisque dans T, les sommets qui sont la source d'une transition étiquetée par 0 sont de degré 1 : on aurait donc $a = b$. On a donc $a, b > 0$. Ainsi,

$$\begin{aligned} \psi(u) = \psi(v) &\implies \psi(w)a\psi(u') = \psi(w)b\psi(v') \\ &\implies a\psi(u') = b\psi(v') \\ &\implies a = b \,, \end{aligned}$$

une contradiction. On en conclut que u et v ne sont pas comparables par la relation $\prec$. Mais puisque l'ordre lexicographique est total (Proposition 1.5), on a soit $u \sqsubseteq v$ ou bien $v \sqsubseteq u$.

Supposons qu'on ait $u \sqsubseteq v$. On peut donc écrire $v = uw$. Or, si w contenait une lettre différente de 0, on aurait $\psi(w) \neq \varepsilon$ et donc $\psi(v) = \psi(u)\psi(w) \neq \psi(u)$, une contradiction. Ainsi donc, $v = u \cdot 0^k$ pour un certain $k \in \mathbb{N}$ et on a terminé. De façon similaire, si $v \sqsubseteq u$, on peut conclure $u = v \cdot 0^j$ pour un certain $j \in \mathbb{N}$. □

Lemme 5.13. *Soit $u, v \in T$. Alors :*

1. *si $u \sqsubseteq v$, alors $\psi(u) \sqsubseteq \psi(v)$;*
2. *si $\psi(u) \sqsubset \psi(v)$, alors $u \sqsubset v$;*
3. *$\psi(u \sqcap v) = \psi(u) \sqcap \psi(v)$;*
4. *$u \prec v$ si et seulement si $\psi(u) \prec \psi(v)$.*

Démonstration.

1. Si $u \sqsubseteq v$, alors on peut écrire $v = uw$. Donc $\psi(u) \sqsubseteq \psi(u)\psi(w) = \psi(v)$.

2. On procède par induction sur v. Le cas $v = \varepsilon$ est trivial, puisque ε n'a pas de préfixe propre. Soit donc $v = wa$ pour $a \in \mathbb{N}$ et $w \in T$. Soit $u \in T$ tel que $\psi(u) \sqsubset \psi(v)$. Si $a = 0$, alors $\psi(v) = \psi(w)$, donc $\psi(u) \sqsubset \psi(w)$ d'où on conclut, par l'hypothèse d'induction, $u \sqsubset w \sqsubset v$. Sinon, $a \in \mathbb{N}$ et donc $\psi(v) = \psi(w)a$, d'où $\psi(u) \sqsubseteq \psi(w)$. Si $\psi(u) \sqsubset \psi(w)$, on peut encore conclure grâce à l'hypothèse d'induction. Si $\psi(u) = \psi(w)$, alors par le Lemme 5.12, ou bien $u \sqsubseteq w \sqsubset v$ et on a terminé, ou sinon, $u = w0^k$ pour un certain $k \in \mathbb{N}$. Mais dans ce cas, si $k > 0$, alors w est la source d'au moins deux transitions dans T : une étiquetée par 0 et une autre par a, ce qui est impossible par construction de T. Ainsi, on a $u = w \sqsubset v$.

3. Si $u \sqsubseteq v$, alors $u \sqcap v = u$. Or, par la partie 1, $\psi(u) \sqsubseteq \psi(v)$, d'où

$$\psi(u) \sqcap \psi(v) = \psi(u) = \psi(u \sqcap v).$$

   Il en va de même du cas $v \sqsubseteq u$. Dans les autres cas, soit $w = u \sqcap v$. Alors il existe $a, b \in \mathbb{N}$ tels que $a \neq b$, $wa \sqsubseteq u$ et $wb \sqsubseteq v$. En particulier, $\deg(w) \geq 2$ d'où on déduit, par construction de T, $a \neq 0$ et $b \neq 0$. Ainsi, par la partie 1,

$$\psi(u) \sqsupseteq \psi(wa) = \psi(w)a \quad \text{et} \quad \psi(v) \sqsupseteq \psi(wb) = \psi(w)b\ .$$

   En particulier, on a $\psi(u) \sqcap \psi(v) = \psi(w)$.

4. Soit $u \prec v$ et $w = u \sqcap v$. Comme dans la démonstration de la partie 3, on peut trouver $a < b$ tels que $\psi(w)a \sqsubseteq \psi(u)$ et $\psi(w)b \sqsubseteq \psi(v)$. En particulier, on a $\psi(u) \prec \psi(v)$.

   Réciproquement, supposons qu'on ait $\psi(u) \prec \psi(v)$. Par la partie 3, on a $\psi(u) \sqcap \psi(v) = \psi(w)$ où $w = u \sqcap v$. Il existe donc $a, b \in \mathbb{N}$ tels que $a < b$, $\psi(w)a \sqsubseteq \psi(u)$ et $\psi(w)b \sqsubseteq \psi(v)$. Par la définition de ψ ainsi que le

Lemme 5.12, il existe donc $j, k \in \mathbb{N}$ tels que $w0^j a \sqsubseteq u$ et $w0^k b \sqsubseteq v$. Puisque w est le plus grand commun préfixe, on doit avoir $j = 0$ ou $k = 0$. Or, si $j < k$, alors $w0^j$ est la source d'au moins deux transitions dans T : une étiquetée par 0 et une autre par a, ce qui est impossible. De la même manière, on ne peut avoir $k < j$, d'où $j = k = 0$. On a donc $wa \sqsubseteq u$ et $wb \sqsubseteq v$, d'où on conclut $u \prec v$. □

La ***trace effective*** est définie comme le langage $\widetilde{T} := \psi(T)$ (comparez les Figures 5.2 et 5.1).

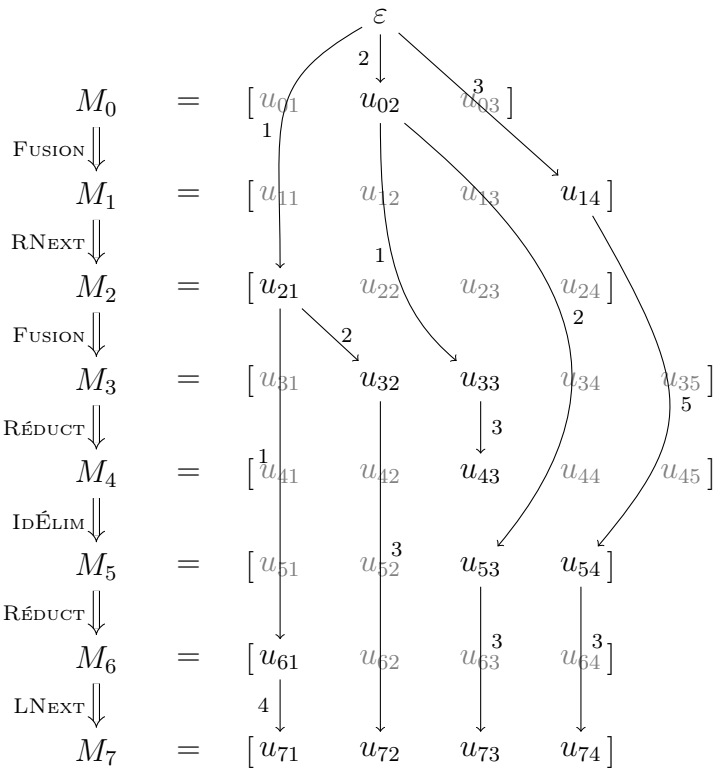


Figure 5.2 Début de la trace effective d'une exécution

Lemme 5.14. *$\widetilde{T}$ est un arbre infini à branchements finis.*

Démonstration. Le fait que $\widetilde{T}$ est un arbre à branchements finis est simplement dû à la correspondance entre arbres et langages décrite à la Section 1.4.

Soit $X = \{n \in \mathbb{N} : M_{n+1} \neq \textsc{IdÉlim}(M_n, i)\}$. Remarquons que X est un ensemble infini car chaque fois où $M_{n+1} = \textsc{IdÉlim}(M_n, i)$, on a $|M_{n+1}| < |M_n|$, mais la suite des $|M_n|$ ne peut décroître indéfiniment puisque $\mathbb{N}$ est bien ordonné. Pour tout $x \in X$, soit $u_x := (x+1, k_x) \in T$ où

$$\begin{aligned} &k_x = 0 \quad \text{si } (x,1) \in P_{\mathtt{L}}, \\ &k_x = |M_x| \quad \text{si } (x, |M_x|) \in P_{\mathtt{R}}, \\ &k_x = i \quad \text{tel que } M_{x+1} = \Phi(M_x, i),\ \Phi \in \{\textsc{Fusion}, \textsc{Réduct}\}, \text{ sinon.} \end{aligned}$$

Par définition de T, on sait que pour tout $x \in X$, la dernière lettre de u_x (rappelons que T est aussi un langage...) n'est pas 0. Toutefois, pour tout $x, y \in X$ tels que $\psi(u_x) = \psi(u_y)$, le Lemme 5.12 nous permet de trouver $w \in T$ et $j, k \in \mathbb{N}$ tels que $u_x = w0^j$ et $u_y = w0^k$. On doit donc avoir $j = k = 0$, d'où $u_x = w = u_y$ et donc $x = y$. On a ainsi montré que la fonction

$$\begin{aligned} f : X &\to \widetilde{T}\,, \\ x &\mapsto \psi(u_x)\,, \end{aligned}$$

est injective. Puisque X est infini, alors $\widetilde{T}$ l'est également. □

Par abus de langage, on peut définir le sommet de la preuve Π correspondant à chaque $v \in \widetilde{T}$. En effet, si $v = \psi(u)$ pour un certain $u \in T$, on pose

$$g(v) := g(u)\ .$$

Lemme 5.15. *La fonction $g : \widetilde{T} \setminus \{\varepsilon\} \to \Pi$ est bien définie.*

Démonstration. On veut montrer que la définition de $g(v)$ ne dépend pas du choix de u. Soit donc $u_1, u_2 \in T$ tels que $\psi(u_1) = v = \psi(u_2)$. Alors par le Lemme 5.12, il

existe $w \in T$ et $j, k \in \mathbb{N}$ tels que $u_1 = w0^j$ et $u_2 = w0^k$. Sans perte de généralité, $j \leq k$ et donc $u_2 = u_1 0^{k-j}$. Par le Lemme 5.9, on conclut $g(u_1) = g(u_2)$. □

Lemme 5.16. *Soit $v \in \widetilde{T} \setminus \{\varepsilon\}$ et $a \in \mathbb{N}$ tel que $va \in \widetilde{T}$. Alors il y a une transition $g(v) \to g(va)$ dans Π.*

Démonstration. Soit $u_1, u_2 \in T$ tels que $\psi(u_1) = v$, $\psi(u_2) = va$. Sans perte de généralité, on peut supposer que la dernière lettre de u_2 n'est pas 0. Ainsi, $u_2 = u_1 0^k a$ pour un certain $k \in \mathbb{N}$. Par définition de LNEXT, RNEXT, FUSION et RÉDUCT, il existe une transition $g(u_1 0^k) \to g(u_2)$ dans Π. Puisque $\psi(u_1 0^k) = \psi(u_1) = v$, alors $g(u_1 0^k) = g(v)$, et puisque $\psi(u_2) = va$, alors $g(u_2) = g(va)$. Il y a donc une transition $g(v) \to g(va)$ dans Π. □

Le dernier Lemme nous permet un rapprochement vers l'exploitation de la condition de garde, puisque les branches infinies de $\widetilde{T}$ correspondent à des chemins infinis dans Π. On s'intéressera donc à étudier les branches infinies de $\widetilde{T}$. Le lecteur est donc avisé d'aller se référer à la Section 1.3 de temps à autre.

Notons d'abord qu'on peut étendre la fonction ψ à ∂T. En effet, soit une chaîne

$$u_1 \sqsubseteq u_2 \sqsubseteq u_3 \sqsubseteq \cdots \in T.$$

Alors par le Lemme 5.13, on a

$$\psi(u_1) \sqsubseteq \psi(u_2) \sqsubseteq \psi(u_3) \sqsubseteq \cdots .$$

On pose alors :

$$\psi\big(\bigsqcup_{n\in\mathbb{N}} u_n\big) := \bigsqcup_{n\in\mathbb{N}} \psi(u_n).$$

Lemme 5.17. *L'extension de ψ à ∂T est bien définie.*

Démonstration. On doit montrer que la définition ne dépend pas de la chaîne choisie dans T. Soit donc $u_1 \sqsubseteq u_2 \sqsubseteq \cdots \in T$ et $u'_1 \sqsubseteq u'_2 \sqsubseteq \cdots \in T$ deux chaînes telles que $\bigsqcup_{n\in\mathbb{N}} u_n = \bigsqcup_{n\in\mathbb{N}} u'_n =: \beta$. Soit $\gamma = \bigsqcup_{n\in\mathbb{N}} \psi(u_n)$ et $\gamma' = \bigsqcup_{n\in\mathbb{N}} \psi(u'_n)$. On veut montrer $\gamma = \gamma'$.

Si γ est fini, alors il y a un certain n_0 tel que $\forall n \geq n_0$, $\psi(u_n) = \gamma$. Par le Lemme 5.12, il existe $v \in T$ tel que $\forall n \geq n_0$, $\exists k_n \in \mathbb{N}$ tel que $u_n = v0^{k_n}$. Il s'ensuit que $\beta = v0^k$ pour un certain $k \in \mathbb{N} \cup \{\omega\}$. En particulier, il existe n_1 tel que $\forall n \geq n_1$, $\exists \ell_n$ tel que $u'_n = v0^{\ell_n}$. Par conséquent, pour tout $n \geq n_1$, $\psi(u'_n) = \psi(v)\psi(0)^{\ell_n} = \psi(v)$, d'où $\gamma' = \psi(v) = \gamma$.

Si c'est plutôt γ' qui est fini, le même raisonnement conduit à la même conclusion, c'est-à-dire $\gamma = \gamma'$.

Supposons donc que γ et γ' sont deux branches infinies et que $\gamma \neq \gamma'$. Alors on ne peut avoir $\gamma \sqsubset \gamma'$ ni l'inverse, puisqu'une branche infinie ne peut être préfixe d'une autre. Soit donc $w = \gamma \sqcap \gamma'$ et soit $a \in \mathbb{N}$ tel que $wa \sqsubset \gamma$. Alors il existe n tel que $wa \sqsubset \psi(u_n)$. Soit $v \in T$ tel que $\psi(v) = wa$. Par la partie 2 du Lemme 5.13, on a $v \sqsubset u_n \sqsubset \beta$. Il existe donc un certain m tel que $v \sqsubseteq u'_m$. Par la partie 1 du Lemme 5.13, $\psi(v) \sqsubseteq \psi(u'_m)$. Donc $wa \sqsubset \gamma'$, mais cela est impossible par maximalité de w. □

Lemme 5.18. *Soit $\gamma \in \partial\widetilde{T}$ une branche infinie. Alors il existe une branche infinie $\beta \in \partial T$ telle que $\gamma = \psi(\beta)$.*

Démonstration. Soit $\gamma = \bigsqcup_{n\in\mathbb{N}} v_n$ où $v_1 \sqsubset v_2 \sqsubset \cdots \in \widetilde{T}$. Pour tout $n \in \mathbb{N}$, soit $u_n \in T$ tel que $\psi(u_n) = v_n$. Par la partie 2 du Lemme 5.13, on a donc $u_1 \sqsubset u_2 \sqsubset \cdots$. Ainsi, la branche $\beta = \bigsqcup_{n\in\mathbb{N}} u_n$ est infinie et on a

$$\psi(\beta) = \psi(\bigsqcup_{n\in\mathbb{N}} u_n) = \bigsqcup_{n\in\mathbb{N}} \psi(u_n) = \bigsqcup_{n\in\mathbb{N}} v_n = \gamma.$$

□

On peut maintenant adapter à $\widetilde{T}$ les résultats préalablement obtenus à propos de T (les Lemmes 5.8, 5.10 et 5.11).

D'abord, par le même abus de langage qu'à l'équation (5.1), on peut définir RÈG sur $\widetilde{T} \setminus \{\varepsilon\}$ par l'équation

$$\text{RÈG}(v) := \text{RÈG}(g(v)) \ .$$

Une ***coupure*** dans $\widetilde{T}$ est un sommet $v \in \widetilde{T}$ tel que $\text{RÈG}(v) = \texttt{C}$. Les ***producteurs*** de $\widetilde{T}$ sont les éléments des ensembles suivants :

$$\widetilde{P}_{\texttt{L}} = \psi(P_{\texttt{L}}) \quad \text{et} \quad \widetilde{P}_{\texttt{R}} = \psi(P_{\texttt{R}}).$$

Lemme 5.19. *Soit γ une branche infinie de $\widetilde{T}$. Alors pour tout $v \in \widetilde{P}_{\texttt{L}}$, ou bien $v \sqsubset \gamma$, ou alors $v \prec \gamma$. De façon similaire, pour tout $v \in \widetilde{P}_{\texttt{R}}$, ou bien $v \sqsubset \gamma$, ou alors $v \succ \gamma$.*

Démonstration. Par le Lemme 5.18, il existe $\beta \in \partial T$ infinie telle que $\psi(\beta) = \gamma$. Soit $v \in \widetilde{P}_{\texttt{L}}$. Donc il existe $u \in P_{\texttt{L}}$ tel que $\psi(u) = v$. Par le Lemme 5.8, ou bien $u \sqsubseteq \beta$, ou alors $u \prec \beta$. En appliquant le Lemme 5.13, qui demeure vrai même en ajoutant les branches infinies, on trouve soit $v \sqsubseteq \gamma$ et donc $v \sqsubset \gamma$ puisque v est un mot fini, ou bien $v \prec \gamma$. Le cas $v \in \widetilde{P}_{\texttt{R}}$ se démontre de la même manière. □

On doit également adapter à $\widetilde{T}$ le concept de ***sommets jumelés***. On le fait encore via la fonction ψ. Soit $v \in \widetilde{T}$ et supposons qu'il existe $u \in T$ jumelé et tel que $\psi(u) = v$. Alors v est un ***sommet jumelé*** et son ***jumeau*** est défini comme suit :

$$\text{jum}(v) := \psi(\text{jum}(u)).$$

Il faut, bien sûr, démontrer que cette définition ne dépend pas du choix de sommet u. Mais en fait, il n'y a aucun choix à effectuer.

Lemme 5.20. *Pour tout $v \in \widetilde{T}$, il existe au plus un sommet jumelé $u \in T$ tel que $\psi(u) = v$.*

Démonstration. Soit $u_1, u_2 \in T$ tels que $\psi(u_1) = v = \psi(u_2)$. Par le Lemme 5.12, il existe $w \in T$ et $j, k \in \mathbb{N}$ tels que $u_1 = w0^j$ et $u_2 = w0^k$. Si $j > 0$, on a donc $u_1 0 \in T$ et alors u_1 n'est pas un sommet jumelé car s'il l'était, $u_1 3$ serait son unique successeur dans T. Il suit donc que $j = 0$ et alors $u_1 = w$. De la même manière, on obtient $u_2 = w$, d'où on conclut $u_1 = u_2$. □

Lemme 5.21. *Pour chaque sommet jumelé $v \in \widetilde{T}$,* $\mathrm{jum}(\mathrm{jum}(v)) = v$ *et on a soit* $v \prec \mathrm{jum}(v)$ *ou bien* $\mathrm{jum}(v) \prec v$.

Démonstration. Soit $v_1 = v$ et soit $u_1 \in T$ l'unique sommet jumelé tel que $\psi(u_1) = v_1$. On pose $u_2 = \mathrm{jum}(u_1)$ et $v_2 = \psi(u_2)$. Alors

$$\mathrm{jum}(v_1) \stackrel{\text{déf}}{=} \psi(\mathrm{jum}(u_1)) = \psi(u_2) = v_2.$$

Or, u_2 est un sommet jumelé de T, d'où on déduit que v_2 est lui-même jumelé et son jumeau n'est nul autre que

$$\mathrm{jum}(v_2) \stackrel{\text{déf}}{=} \psi(\mathrm{jum}(u_2)) = \psi(\mathrm{jum}(\mathrm{jum}(u_1))) = \psi(u_1) = v_1.$$

On a donc

$$\mathrm{jum}(\mathrm{jum}(v_1)) = \mathrm{jum}(v_2) = v_1.$$

Pour l'autre partie, remarquons d'abord que $v_1 \neq v_2$, car si $v_1 = v_2$, alors par unicité, on aurait $u_1 = u_2$ ce qui est impossible. De plus, si $v_1 \sqsubset v_2$ ou $v_2 \sqsubset v_1$, alors par le Lemme 5.13, ou bien $u_1 \sqsubset u_2$ ou alors $u_2 \sqsubset u_1$ ce qui est, encore une fois, faux. Puisque l'ordre lexicographique est total, on conclut qu'on a soit $v_1 \prec v_2$ ou bien $v_2 \prec v_1$. □

Lemme 5.22. *Soit $v_1, v_2 \in \widetilde{T}$ des jumeaux. Alors $v_1 \prec v_2$ si et seulement si l'une des situations suivantes se produit :*

- $\text{RÈG}(v_1) = \texttt{R}\times$ *et* $\text{RÈG}(v_2) = \texttt{L}\times_j$ *où* $j \in \{0, 1\}$ *;*
- $\text{RÈG}(v_1) = \texttt{R}+_j$ *et* $\text{RÈG}(v_2) = \texttt{L}+$ *où* $j \in \{0, 1\}$ *;*
- $\text{RÈG}(v_1) = \texttt{RF}_X$ *et* $\text{RÈG}(v_2) = \texttt{LF}_X$ *où* $X \in \mathsf{BV}(S)$.

Démonstration. Soit $u_1, u_2 \in T$ les uniques sommets jumelés tels que $\psi(u_1) = v_1$ et $\psi(u_2) = u_1$. Alors, par unicité, $\text{jum}(u_1) = u_2$ et $\text{jum}(u_2) = u_1$. Par les Lemmes 5.13 et 5.21, on sait que $v_1 \prec v_2$ si et seulement si $u_1 \prec u_2$. De plus, remarquons qu'on a $\text{RÈG}(u_1) = \text{RÈG}(v_1)$ et $\text{RÈG}(u_2) = \text{RÈG}(v_2)$. La conclusion découle donc d'une simple substitution dans l'énoncé du Lemme 5.10. □

Lemme 5.23. *Soit γ une branche infinie de $\widetilde{T}$ et soit $v \in \widetilde{T}$ un sommet jumelé. Alors :*

1. *si $v \prec \gamma$, alors soit* $\text{jum}(v) \prec \gamma$ *ou bien* $\text{jum}(v) \sqsubset \gamma$;
2. *si $v \succ \gamma$, alors soit* $\text{jum}(v) \succ \gamma$ *ou bien* $\text{jum}(v) \sqsubset \gamma$.

Démonstration. Il suffit de démontrer le cas 1, le cas 2 lui étant similaire. Soit $u \in T$ le sommet jumelé tel que $v = \psi(u)$. Par le Lemme 5.18, il existe une branche infinie $\beta \in \partial T$ telle que $\psi(\beta) = \gamma$. Ainsi, puisque $v \prec \gamma$, alors par le Lemme 5.13, on a $u \prec \beta$. Il découle alors du Lemme 5.11 qu'on a soit $\text{jum}(u) \prec \beta$ ou bien $\text{jum}(u) \sqsubset \beta$. Puisque $\text{jum}(v) = \psi(\text{jum}(u))$, alors par le Lemme 5.13, on conclut qu'on a soit $\text{jum}(v) \prec \beta$ ou bien $\text{jum}(v) \sqsubset \beta$. □

En passant de T à $\widetilde{T}$ on a, en apparence, perdu un avantage à propos de la position des sommets, en ce sens qu'on ne peut plus reposer sur leur description en tant qu'éléments de $\mathbb{N} \times \mathbb{N}$ pour démontrer des propriétés. On a toutefois gagné un précieux avantage pour ce qui est de localiser les sommets importants : les coupures, les producteurs et les sommets jumelés.

Lemme 5.24. *Soit $v \in \widetilde{T}$. Alors il y a seulement cinq possibilités, mutuellement exclusives :*

1. *$v = \varepsilon$, la racine de $\widetilde{T}$;*
2. *v est une feuille, c'est-à-dire un sommet de degré 0 ;*
3. *v est une coupure, de degré 2 ;*
4. *v est un producteur, de degré 1 ;*
5. *v est un sommet jumelé, de degré 1.*

Démonstration. Remarquons d'abord que ε n'est pas une feuille (car $\widetilde{T}$ est infini), ni une coupure (puisque $\text{RÈG}(\varepsilon)$ n'est pas défini), ni un producteur ou un sommet jumelé (car le seul $u \in T$ tel que $\psi(u) = \varepsilon$ est $u = *$, qui n'appartient à aucun des M_n). Soit donc $v \neq \varepsilon$. Si v est un sommet de degré 1 ou 2, alors il n'est pas de degré 0, donc pas une feuille.

Réciproquement, supposons que v n'est pas une feuille. Donc il existe $a \in \mathbb{N}$ tel que $va \in \widetilde{T}$. Soit $u \in T$ tel que $\psi(u) = va$ et $w \in T$ tel que $\psi(w) = v$. Alors $u = w0^j a0^k$ pour certains $j, k \in \mathbb{N}$. Soit $w' = w0^j$. Donc $\psi(w') = v$. Si $a \in \{1, 2\}$, alors $\text{RÈG}(v) = \text{RÈG}(w') = \texttt{C}$ et $\deg(v) = \deg(w') = 2$. Si $a = 3$, alors w' est un sommet jumelé de degré 1 et donc v est lui-même un sommet jumelé du même degré. Enfin, si $a \in \{4, 5\}$, alors w' est un producteur et donc v aussi. Il est clair, de la définition de T, que ces trois dernières situations sont mutuellement exclusives. □

5.5 Branches spéciales

Notre premier objectif est d'énoncer ce qu'implique la condition de garde pour les branches infinies de $\widetilde{T}$. Soit $\beta \in \partial\widetilde{T}$. On peut définir les propriétés μ et ν de façon analogue à ce qu'on a fait à la Section 3.4, c'est-à-dire, en considérant les deux

ensembles suivants.

$$\begin{aligned} L^\infty(\beta) &:= \{p_X : X \in \mathsf{BV}(\mathcal{S}) \text{ et } \exists^\infty u \sqsubset \beta \text{ t.q. } \text{RÈG}(u) = \mathtt{LF}_X\}; \\ R^\infty(\beta) &:= \{p_X : X \in \mathsf{BV}(\mathcal{S}) \text{ et } \exists^\infty u \sqsubset \beta \text{ t.q. } \text{RÈG}(u) = \mathtt{RF}_X\}. \end{aligned} \tag{5.2}$$

On dit que β a ***la propriété μ*** si $L^\infty(\beta) \neq \varnothing$ et $\max(L^\infty(\beta))$ est un nombre impair. Symétriquement, on dit que β a ***la propriété ν*** si $R^\infty(\beta) \neq \varnothing$ et $\max(R^\infty(\beta))$ est un nombre pair. Une coupure $u \sqsubset \beta$ est dite ***β-gauche*** si $u{\cdot}1 \sqsubseteq \beta$ et ***β-droite*** si $u \cdot 2 \sqsubseteq \beta$.

On dit qu'une branche infinie β est une ***μ-branche*** si elle a la propriété μ et si peut écrire $\beta = \beta_0 \cdot \beta_1$ où chaque règle de point fixe utilisée dans β_1 y est utilisée infiniment souvent et chaque coupure v telle que $\beta_0 \sqsubseteq v \sqsubset \beta$ est une coupure β-gauche. Similairement, β est une ***ν-branche*** si elle a la propriété ν et si on peut écrire $\beta = \beta_0 \cdot \beta_1$ où chaque règle de point fixe utilisée dans β_1 y est utilisée infiniment souvent et chaque coupure v telle que $\beta_0 \sqsubseteq v \sqsubset \beta$ est une coupure β-droite.

En particulier, on remarque que si β est une μ-branche, alors elle a seulement un nombre fini de coupures β-droites comme préfixe. Dualement, si β est une ν-branche, alors elle a seulement un nombre fini de coupures β-gauches comme préfixe.

Lemme 5.25. *Si Π est une preuve circulaire, alors toute branche infinie de $\widetilde{T}$ est soit une μ-branche, soit une ν-branche.*

Démonstration. Soit $\beta \in \partial\widetilde{T}$ une branche infinie. On peut lui faire correspondre un chemin canonique Γ dans Π dont les sommets sont donnés par l'équation

$$\Gamma(n) = g(\beta \restriction_n)$$

et les transitions entre sommets consécutifs sont fournies par le Lemme 5.16. Puisque β est infinie et puisque chacune de ses transitions correspond à une tran-

sition dans Π, alors Γ est un chemin infini. Ainsi, puisque Π satisfait la condition de garde **G2**, on peut écrire $\Gamma = \Gamma_0 \cdot \Gamma_1$ de façon à ce que Γ_1 ait une μ-trace gauche ou une ν-trace droite et chaque règle de point fixe dans Γ_1 soit utilisée infiniment souvent.

Supposons que Γ_1 ait une μ-trace gauche (le cas de la ν-trace droite lui est symétrique). Par le Lemme 3.2, il existe $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$, si $\text{RÈG}(\Gamma(n)) = \mathtt{C}$, alors

$$\Gamma(n+1) = \varsigma_0 \Gamma(n) \; . \tag{5.3}$$

Soit $\beta_0 = \beta \restriction_m$, où $m = \max\{n_0, |\Gamma_0|\}$ et soit β_1 le suffixe de β tel que $\beta = \beta_0 \cdot \beta_1$. Le fait que Γ_1 ait une μ-trace gauche implique directement que β a la propriété μ et que chaque règle de point fixe qui y est utilisée l'est une infinité de fois. Il ne reste donc qu'à démontrer que pour toute coupure $v \in \widetilde{T}$ telle que $\beta_0 \sqsubseteq v \sqsubset \beta$, on a $v1 \sqsubset \beta$.

Soit donc un tel v et soit $n = |v|$. Soit $\beta \restriction_{n+1} = v \cdot a$. Puisque $va \in \widetilde{T}$, alors $a \neq 0$. Regardons de nouveau comment la transition $g(v) \to g(va)$ est définie dans la démonstration du Lemme 5.16. On doit choisir $u_1, u_2 \in T$ tels que $\psi(u_1) = v$ et $u_2 = u_1 a$ (donc $\psi(u_2) = va$). Soit $m, i, j \in \mathbb{N}$ tels que $(m, i) = u_1$ et $(m+1, j) = u_2$. Puisque $\text{RÈG}(u_1) = \text{RÈG}(v) = \mathtt{C}$ et puisque $u_1 \xrightarrow{a} u_2$ avec $a \neq 0$, alors par construction de T, on doit avoir $M_{m+1} = \textsc{Fusion}(M_m, i)$. Par la définition de FUSION, on a donc $a \in \{1, 2\}$ avec

$$\begin{aligned} a = 1 &\iff j = i \text{ et } g(u_2) = \varsigma_0 g(u_1) \; ; \\ a = 2 &\iff j = i+1 \text{ et } g(u_2) = \varsigma_1 g(u_1) \; . \end{aligned}$$

Or, puisque $n \geq m \geq n_0$, alors en appliquant l'équation (5.3), on trouve $a = 1$, d'où on conclut $v1 \sqsubset \beta$. □

Proposition 5.26. *Soit E une collection non vide de ν-branches et soit $\gamma = \bigvee E$. Alors γ est une ν-branche.*

Démonstration. Si $\gamma \in E$, alors par hypothèse, γ est une ν-branche et on a terminé. Supposons donc $\gamma \notin E$. Alors par le Lemme 1.9, il existe une chaîne

$$\beta_0 \prec \beta_1 \prec \beta_2 \prec \ldots \in E$$

telle que $\gamma = \bigsqcup_{i\in\mathbb{N}} u_i$, où $u_i = \beta_i \sqcap \beta_{i+1}$ et $u_i \sqsubset u_{i+1}$ pour tout i.

Soit $i > 0$. Alors $u_i \neq \varepsilon$ et puisque $u_i = \beta_i \sqcap \beta_{i+1}$ il s'ensuit que $\deg(u_i) \geq 2$. Par le Lemme 5.24, u_i est donc une coupure, d'où il découle, par construction de $\widetilde{T}$, qu'on a $u_i 1 \sqsubset \beta_i$ et $u_i 2 \sqsubset \beta_{i+1}$. Or, on a aussi $u_{i+1} \sqsubset \beta_{i+1}$. Puisque $u_{i+1} \not\sqsubset u_i 2$ (cela contredirait $u_i \sqsubset u_{i+1}$), alors le Lemme 1.2 nous permet d'obtenir $u_i 2 \sqsubseteq u_{i+1}$. Ainsi, $u_i 2 \sqsubset \gamma$ et u_i est donc une coupure γ-droite. Puisque cela est vrai pour tous les $i > 0$, on conclut que γ est suffixe d'une infinité de coupures γ-droites. Il ne s'agit donc pas d'une μ-branche et alors, par le Lemme 5.25, γ est une ν-branche. □

Corollaire 5.27. *Soit E une collection non vide de μ-branches et soit $\gamma = \bigwedge E$. Alors γ est une μ-branche.*

Démonstration. C'est l'énoncé dual de la Proposition 5.26. □

Parmi toutes les branches infinies de $\widetilde{T}$, deux sont particulières : la plus petite et la plus grande (qui existent par le Lemme 1.8). On dénote par $\lambda_{\mathtt{L}}$ la branche infinie minimale et par $\lambda_{\mathtt{R}}$ la branche infinie maximale.

Lemme 5.28. *Si $|\widetilde{P}_{\mathtt{R}}| = \infty$, alors $\lambda_{\mathtt{R}}$ est la seule branche à contenir une infinité de $v \in \widetilde{P}_{\mathtt{R}}$. Dans ce cas, on dira que $\lambda_{\mathtt{R}}$ est* **active**.

Démonstration. Soit $\Lambda = {\downarrow}\widetilde{P}_{\mathtt{R}}$. Par minimalité, on a $\Lambda \subseteq \widetilde{T}$. Puisque $\widetilde{P}_{\mathtt{R}}$ est infini, alors Λ est infini et donc, par le Lemme de Kőnig, Λ admet au moins une branche infinie, qu'on dénote λ. Trivialement, on a $\lambda \preceq \lambda_{\mathtt{R}}$.

Or, par minimalité de Λ, λ doit avoir une infinité de $v \in \widetilde{P}_{\mathtt{R}}$ comme préfixes. On a donc

$$\lambda = \bigsqcup_{n\in\mathbb{N}} v_n$$

où, pour tout n, $v_n \in \widetilde{P}_{\mathtt{R}}$. Or, par le Lemme 5.19 (avec $\gamma = \lambda_{\mathtt{R}}$), pour tout n, on a $v_n \succ \lambda_{\mathtt{R}}$ ou $v_n \sqsubseteq \lambda_{\mathtt{R}}$. Mais le cas $v_n \succ \lambda_{\mathtt{R}}$ ne peut pas se produire, car si c'était le cas, il existerait $w \in \Lambda$ et $a, b \in \mathbb{N}$ tels que $a < b$, $wa \sqsubset \lambda_{\mathtt{R}}$ et $wb \sqsubseteq v_n \sqsubset \lambda$. On aurait alors la contradiction $\lambda_{\mathtt{R}} \prec \lambda$.

Ainsi, pour tout n, on a $v_n \sqsubseteq \lambda_{\mathtt{R}}$, d'où $\lambda = \bigsqcup_{n\in\mathbb{N}} v_n \sqsubseteq \lambda_{\mathtt{R}}$. Mais puisqu'une branche infinie ne peut être un préfixe (propre) d'une autre, alors $\lambda = \lambda_{\mathtt{R}}$. □

Corollaire 5.29. *Si $|\widetilde{P}_{\mathtt{L}}| = \infty$, alors $\lambda_{\mathtt{L}}$ est la seule branche à contenir une infinité de $v \in \widetilde{P}_{\mathtt{L}}$. Dans ce cas, on dira que $\lambda_{\mathtt{L}}$ est* **active**.

Démonstration. C'est l'énoncé dual à celui du Lemme 5.28. □

Proposition 5.30. *Soit β une ν-branche. Alors ou bien $\lambda_{\mathtt{R}}$ est active et $\beta = \lambda_{\mathtt{R}}$, ou sinon, il existe une autre ν-branche $\gamma \succ \beta$.*

Démonstration. Puisque β est une ν-branche, alors il y a seulement un nombre fini de coupures β-gauches, disons $u_1 \sqsubset u_2 \sqsubset \cdots \sqsubset u_n$. De plus, la propriété ν implique qu'il existe une infinité de $p \sqsubset \beta$ tels que $\text{RÈG}(p) \in \mathfrak{R}$.

Supposons que $\beta \neq \lambda_{\mathtt{R}}$ ou que $\lambda_{\mathtt{R}}$ est inactive. Dans les deux cas, le Lemme 5.28 implique qu'il existe seulement un nombre fini de $v \sqsubset \beta$ appartenant à $\widetilde{P}_{\mathtt{R}}$. Par le Lemme 5.24, tous les autres $p \sqsubset \beta$ tels que $\text{RÈG}(p) \in \mathfrak{R}$ sont des sommets jumelés. Il y en a donc une infinité, dont la liste complète est dénotée $p_1 \sqsubset p_2 \sqsubset p_3 \sqsubset \cdots$.

Pour chaque p_i, le Lemme 5.22 implique $\text{jum}(p_i) \succ \beta$. Il existe donc $a, b \in \mathbb{N}$ et $w \sqsubset \beta$ tels que $a < b$, $wa \sqsubset \beta$ et $wb \sqsubseteq \text{jum}(p_i)$. Par le Lemme 5.24, il y a seulement deux possibilités pour les identités de w, a et b :

1. $w = \varepsilon$, $a = \beta\restriction_1$ et $a < b < \deg(\varepsilon)$;
2. w est une coupure, donc $w = u_j$ pour un $j \in [1 \dots n]$, $a = 1$ et $b = 2$.

Soit les ensembles suivants :

$$W_0 = \{w \in \widetilde{T} : \beta\restriction_1 < w\restriction_1\},$$
$$W_j = \{w \in \widetilde{T} : u_j 2 \sqsubseteq w\} \qquad (1 \leq j \leq n).$$

On a donc, pour tout i, $\mathrm{jum}(p_i) \in \bigcup_{j=0}^{n} W_j$. Par le principe des nids de pigeons, il existe au moins un j tel que W_j est infini. Soit j_0 le plus grand tel j, et soit γ la branche infinie minimale de W_j (qui existe par le Lemme 1.8). On a immédiatement $\beta \prec \gamma$ et on veut montrer que γ est une ν-branche.

Supposons le contraire. Par le Lemme 5.25, γ est donc μ-branche. Puisque $\beta \prec \gamma$, alors $\gamma \neq \lambda_{\mathrm{L}}$. On peut donc répéter le même argumentaire que plus haut (dualisé) pour conclure qu'il existe seulement un nombre fini de coupures γ-droites, disons $v_1 \sqsubset v_2 \sqsubset \cdots \sqsubset v_m$, et une quantité infinie de sommets jumelés $q \sqsubset \gamma$ tels que $\textsc{Règ}(q) \in \mathfrak{L}$, dont la liste complète est dénotée $q_1 \sqsubset q_2 \sqsubset q_3 \sqsubset \cdots$.

Montrons qu'il y a seulement une quantité finie de sommets $w \in \widetilde{T}$ tels que $\beta \prec w \prec \gamma$. Il y a, en effet, seulement trois possibilités concernant un tel w :

1. $w \in W_j$ où $j > j_0$. Or, cela ne peut se produire qu'un nombre fini de fois par maximalité de j_0.
2. $\exists v_k \in W_{j_0}$ tel que $v_k 1 \sqsubseteq w$. Mais si cela devait se produire une infinité de fois, on pourrait trouver un certain k_0 tel que l'ensemble $\{w \in \widetilde{T} : v_k 1 \sqsubseteq w\}$ est infini. Par le Lemme de Kőnig, il y aurait donc une branche infinie α telle que $v_{k_0} 1 \sqsubset \alpha$. Mais alors, α serait une branche infinie de W_{j_0} inférieure à γ, ce qui contredirait la minimalité de cette dernière.
3. $j_0 = 0$ et $\beta\restriction_1 < w\restriction_1 < \gamma\restriction_1$. Mais si cela devait se produire une infinité de fois, on pourrait trouver $a \in \mathbb{N}$ tel que $\beta\restriction_1 < a < \gamma\restriction_1$ et l'ensemble

$\{w \in \widetilde{T} : a \sqsubseteq w\}$ est infini. Encore une fois, grâce au Lemme de Kőnig, on pourrait alors trouver une branche infinie α telle que $a \sqsubseteq \alpha$, contredisant la minimalité de γ.

Par le Lemme 5.23, on sait que pour tout i, ou bien $\beta \prec \mathrm{jum}(p_i) \prec \gamma$, ou alors $\mathrm{jum}(p_i) \sqsubset \gamma$. Puisque la première de ces éventualités ne peut se produire qu'un nombre fini de fois, alors $\exists i_0 \in \mathbb{N}$ tel que $\forall i \geq i_0$, $\mathrm{jum}(p_i) \sqsubset \gamma$. Dans ce cas, il existe un indice j tel que $\mathrm{jum}(p_i) = q_j$. De façon similaire, $\exists i_1 \in \mathbb{N}$ tel que $\forall i \geq i_1$, il existe un indice j tel que $\mathrm{jum}(q_i) = p_j$.

Puisque β est une ν-branche, la propriété ν indique qu'il existe une variable $X \in \mathsf{BV}(\mathcal{S})$ telle que p_X est un nombre pair et $\text{RÈG}(p_i) = \mathtt{RF}_X$ pour une infinité d'indices i. De plus, X est maximale, en ce sens que pour toute autre variable $Z \in \mathsf{BV}(\mathcal{S})$ telle que $\text{RÈG}(p_i) = \mathtt{RF}_Z$ pour une infinité de i, on doit avoir $p_Z \leq p_X$. Notons que par le Lemme 5.22 et le paragraphe précédent, il existe une infinité d'indices j tels que $\text{RÈG}(q_j) = \mathtt{LF}_X$.

De façon similaire, puisque γ est une μ-branche, la propriété μ indique qu'il existe une variable $Y \in \mathsf{BV}(\mathcal{S})$ telle que p_Y est un nombre impair et $\text{RÈG}(q_j) = \mathtt{LF}_Y$ pour une infinité d'indices j. De plus, Y est maximale, en ce sens que pour toute autre variable $Z \in \mathsf{BV}(\mathcal{S})$ telle que $\text{RÈG}(q_j) = \mathtt{LF}_Z$ pour une infinité d'indices j, on doit avoir $p_Z \leq p_Y$. En particulier, $p_X \leq p_Y$ et puisque p_X et p_Y n'ont pas la même parité, on trouve $p_X < p_Y$.

Mais encore une fois, par le Lemme 5.22 et la discussion ci-haut, il existe une infinité d'indices i tels que $\text{RÈG}(p_i) = \mathtt{RF}_Y$, d'où on conclut $p_Y \leq p_X$: une contradiction. □

Corollaire 5.31. *Soit β une μ-branche. Alors ou bien $\lambda_{\mathtt{L}}$ est active et $\beta = \lambda_{\mathtt{L}}$, ou sinon, il existe une autre μ-branche $\gamma \prec \beta$.*

Démonstration. C'est l'énoncé dual à celui de la Proposition 5.30. □

Proposition 5.32. *Ou bien $\lambda_{\mathtt{L}}$ est active est c'est une μ-branche, ou alors $\lambda_{\mathtt{R}}$ est active et c'est une ν-branche.*

Démonstration. Puisque $\widetilde{T}$ est infini, alors par le Lemme de Kőnig, il existe une branche $\beta_0 \in \partial\widetilde{T}$ infinie. Par le Lemme 5.25, β_0 est soit une ν-branche ou bien une μ-branche.

Supposons que β_0 est une ν-branche. Alors la collection E de toutes les ν-branches de $\widetilde{T}$ est non vide. Soit $\gamma = \bigvee E$. Par la Proposition 5.26, γ est une ν-branche. Puisqu'il n'existe aucune ν-branche $\gamma' \succ \gamma$, alors par la Proposition 5.30, on conclut que $\lambda_{\mathtt{R}}$ est active et $\gamma = \lambda_{\mathtt{R}}$. Donc $\lambda_{\mathtt{R}}$ est une ν-branche.

De façon duale, si β_0 est une μ-branche, alors la collection E de toutes les μ-branches de $\widetilde{T}$ est non vide. Soit $\gamma = \bigwedge E$. Par le Corollaire 5.27, γ est une μ-branche. Puisqu'il n'existe aucune μ-branche $\gamma' \prec \gamma$, alors par le Corollaire 5.31, on conclut que $\lambda_{\mathtt{L}}$ est active et $\gamma = \lambda_{\mathtt{L}}$. Donc $\lambda_{\mathtt{L}}$ est une μ-branche. □

Corollaire (Théorème 5.1)**.** *Si* Π *satisfait la condition de garde, alors il n'existe aucune* $\bowtie$*-chaîne infinie dans* $\mathcal{M}_\Pi$*.*

Démonstration. Comme on en a fait la remarque à la Section 5.3, ce résultat est équivalent à affirmer qu'on a nécessairement $P_{\mathtt{L}} \cup P_{\mathtt{R}} \neq \varnothing$. Mais cela est, à son tour, équivalent à affirmer $\widetilde{P}_{\mathtt{L}} \cup \widetilde{P}_{\mathtt{R}} \neq \varnothing$. Or, la Proposition 5.32 implique qu'on a soit $|\widetilde{P}_{\mathtt{L}}| = \infty$ ou $|\widetilde{P}_{\mathtt{R}}| = \infty$. On a donc, $|\widetilde{P}_{\mathtt{L}} \cup \widetilde{P}_{\mathtt{R}}| = \infty$, ce qui conclut la preuve. □

Comme promis, les outils développés pour démontrer le Théorème 5.1 nous permettront également, dans un instant, de démontrer le Théorème 5.6. Mais d'abord, un dernier brin de terminologie. Rappelons qu'on interprète la suite $(M_n)_{n\in\mathbb{N}}$ de

multicoupures comme représentant les états successifs de la mémoire d'un automate qui construit *une* branche infinie de la pré-preuve $\textsc{ce}_\Pi(M)$. Appelons cette branche λ et soit Λ l'ensemble des préfixes finis de λ. Les seuls instants où l'automate construit un morceau de λ sont lorsqu'il utilise les opérations LNext et RNext pour modifier sa mémoire. On a donc une bijection :

$$f : P_{\mathtt{L}} \cup P_{\mathtt{R}} \to \Lambda$$

telle que, pour tout $u \in P_{\mathtt{L}} \cup P_{\mathtt{R}}$, $\textsc{Règ}(u) = \textsc{Règ}(f(u))$. Remarquons d'ailleurs, avec l'aide du Lemme 5.12 que $\psi \restriction_{P_{\mathtt{L}} \cup P_{\mathtt{R}}}$ est une bijection. En posant $\widetilde{f} = \psi^{-1} \cdot f$, on a donc une bijection :

$$\widetilde{f} : \widetilde{P}_{\mathtt{L}} \cup \widetilde{P}_{\mathtt{R}} \to \Lambda$$

telle que, pour tout $v \in \widetilde{P}_{\mathtt{L}} \cup \widetilde{P}_{\mathtt{R}}$, $\textsc{Règ}(v) = \textsc{Règ}(\widetilde{f}(v))$.

Lemme 5.33. *Si $\lambda_{\mathtt{R}}$ est active et si c'est une ν-branche de $\widetilde{T}$, alors λ satisfait la propriété ν.*

Démonstration. Puisque $\lambda_{\mathtt{R}}$ est une ν-branche, alors il existe un nombre fini de coupures $\lambda_{\mathtt{R}}$-gauches. Ainsi, et puisque $\lambda_{\mathtt{R}}$ est la branche infinie maximale de $\widetilde{T}$, alors il existe seulement un nombre fini de sommets $v \in \widetilde{T}$ tels que $v \succ \lambda_{\mathtt{R}}$. Il ne peut donc y avoir qu'une quantité finie de sommets jumelés $u \sqsubset \lambda_{\mathtt{R}}$ tels que $\textsc{Règ}(u) \in \mathfrak{R}$, puisque pour chacun, on a $\mathrm{jum}(u) \succ \lambda_{\mathtt{R}}$ par le Lemme 5.22. Il s'ensuit, grâce au Lemme 5.24 qu'il existe $w \sqsubset \lambda_{\mathtt{R}}$ tel que $\forall u$, si $w \sqsubseteq u \sqsubset \lambda_{\mathtt{R}}$ et $\textsc{Règ}(u) \in \mathfrak{R}$, alors $u \in \widetilde{P}_{\mathtt{R}}$. Soit donc $W = \{u \in \widetilde{T} : w \sqsubseteq u \sqsubset \lambda_{\mathtt{R}}\}$.

Ainsi, chaque règle $\mathtt{RF}_X$ utilisée infiniment souvent dans $\lambda_{\mathtt{R}}$ est également utilisée infiniment souvent dans W et donc aussi dans $\widetilde{f}(W) \subseteq \Lambda$. Le fait que $\lambda_{\mathtt{R}}$ satisfasse la propriété ν (telle que définie à la présente section) implique donc que λ satisfait la propriété ν (telle que définie à la Section 3.4). □

Lemme 5.34. *Si λ_{L} est active et si c'est une μ-branche de $\widetilde{T}$, alors λ satisfait la propriété μ.*

Démonstration. C'est l'énoncé dual à celui du Lemme 5.33. □

Corollaire (Théorème 5.6)**.** *Si* Π *satisfait la condition de garde, alors pour tout $M \in \mathcal{M}_\Pi$, la pré-preuve $\mathrm{CE}_\Pi(M)$ satisfait elle-même la condition de garde sur les chemins infinis.*

Démonstration. Puisque $\mathrm{CE}_\Pi(M)$ est, par construction, une pré-preuve sans coupures, alors la condition de garde se reformule comme suit : chaque chemin infini dans $\mathrm{CE}_\Pi(M)$ satisfait la propriété μ ou la propriété ν. Puisque $\mathrm{CE}_\Pi(M)$ est un arbre, ses chemins infinis correspondent à ses branches infinies. Or, chaque branche infinie λ correspond à une suite de multicoupures $(M_n)_{n\in\mathbb{N}}$ avec laquelle on peut refaire le travail des Sections 5.3 à 5.5. La Proposition 5.32 couplée aux Lemmes 5.33 et 5.34 permet alors d'obtenir le résultat voulu à propos de λ. □

CHAPITRE VI

SÉMANTIQUE OPÉRATIONNELLE

Au Chapitre 4, on a montré que les preuves circulaires dénotaient pleinement les flèches de la catégorie μ-bicomplète libre. Dans la catégorie des ensembles, les flèches ainsi représentées sont simplement des fonctions. Dans le présent chapitre, on démontre que l'élimination des coupures peut être utilisée comme une méthode générale pour *calculer* ces fonctions. L'élimination des coupures est ainsi une sémantique *opérationnelle* des preuves circulaires, qui généralise leur sémantique dénotationnelle. Le travail technique derrière une telle affirmation passe par la sémantique des preuves arborescentes, possiblement infinies.

6.1 Preuves arborescentes

À la section 5.2, on a défini qu'une pré-preuve Ψ était dite ***arborescente*** si son support était un arbre (possiblement infini). On dénote indistinctement la racine d'une telle pré-preuve par le symbole ε. Le premier cas de figure est, bien sûr, une pré-preuve de la forme $\mathrm{CE}_\Pi(M)$ où Π est une preuve circulaire et $M \in \mathcal{M}_\Pi$. Dans cette section, on développe plus en profondeur la théorie des *preuves* arborescentes.

Comme pour les preuves circulaires, les preuves arborescentes sont des pré-preuves qui satisfont une certaine condition de garde. Celle-ci est simplement une adaptation de la condition de garde **G2** des preuves circulaires (sur les chemins infinis),

à l'exception du fait que le concept de coupure gauche ou droite n'a plus de sens, puisqu'il n'y a pas de cycles dans une preuve arborescente.

Soit donc Ψ une pré-preuve arborescente et soit Γ un chemin infini dans Ψ. Les propriétés μ et ν sont définies comme à la Section 3.4. Une coupure $u \in \Psi$ est dite **Γ-*gauche*** s'il existe $n \in \mathbb{N}$ tels que $\Gamma(n) = u$ et $\Gamma(n+1) = \varsigma_0 u$. Similairement, une coupure $u \in \Psi$ est dite **Γ-*droite*** s'il existe $n \in \mathbb{N}$ tels que $\Gamma(n) = u$ et $\Gamma(n+1) = \varsigma_1 u$. Ces deux situations sont mutuellement exclusives car chaque sommet visité par Γ n'est visité qu'une seule fois.

Ainsi, on dira que Γ a une ***μ-trace gauche*** s'il a la propriété μ et s'il n'existe aucune coupure Γ-droite. Symétriquement, Γ a une ***ν-trace droite*** si Γ a la propriété ν et s'il n'existe aucune coupure Γ-gauche. On peut maintenant formuler la condition de garde.

Condition de garde (Pour les preuves arborescentes)**.** *Chaque chemin infini Γ de Ψ peut être factorisé en $\Gamma = \Gamma_0 \cdot \Gamma_1$ où Γ_0 est fini, Γ_1 a soit une μ-trace gauche ou une ν-trace droite, et chaque règle de point fixe utilisée dans Γ_1 y est utilisée infiniment souvent.*

Ainsi, une ***preuve arborescente*** est une pré-preuve arborescente Ψ satisfaisant la condition de garde. Si Ψ est sans coupure, alors clairement, cette dernière condition est équivalente à la condition de garde **G2** de la Section 3.4. En particulier, par le Théorème 5.6, les pré-preuves de la forme $\textsc{ce}_\Pi(M)$, où Π est une preuve circulaire, sont des preuves arborescentes au sens de la présente définition.

Lemme 6.1. *Soit Ψ une preuve arborescente sans coupures sur un système d'équations $\mathcal{S}$ tel que, pour tout $X \in \mathcal{S}$, p_X est impair (μ). Alors Ψ est une preuve finie.*

Démonstration. Supposons, au contraire, que Ψ est infinie. Puisque son support

est un arbre, alors le Lemme de Kőnig (1.8) assure qu'il existe une branche infinie $\lambda \in \partial\Psi$. Or, par la condition de garde, λ a soit la propriété μ, soit la propriété ν.

Puisque Ψ est sans coupures, alors par le Lemme 5.4, toutes les règles utilisées dans λ sont des règles droites. Donc λ n'a pas la propriété μ, puisque celle-ci exige l'utilisation d'une règle gauche.

D'un autre côté, si λ a la propriété ν, alors il devait y avoir une variable $X \in \mathcal{S}$ telle que la règle $\mathtt{RF}_X$ est utilisée dans λ et p_X est pair. Mais par hypothèse, la priorité de chacune des variables de $\mathcal{S}$ est impaire : une contradiction. □

Démontrons l'adéquation des preuves arborescentes sans coupures dont la partie gauche du séquent à la racine (et donc de tous ses séquents, par le Lemme 5.4), dans la catégorie des ensembles. Elles peuvent être interprétées comme dénotant les éléments des ensembles définissables par les systèmes dirigés d'équations.

Rappelons que si Ψ est une preuve arborescente sans coupures ni identités, alors Ψ est homogène au sens de la Section 4.2. Comme son système naturel d'équations ne dépend d'aucune collection β de transformations naturelles (car il n'y a pas de coupures), on le dénotera simplement $[\mathbf{?}\Psi]^{\mathcal{S}}$ et sa solution sera dénotée $[\mathbf{!}\Psi]^{\mathcal{S}}$.

Proposition 6.2. *Soit Ψ une preuve arborescente sans coupures ni identités sur un système dirigé $\mathcal{S}$ telle que $\textsc{Seq}_{\mathtt{L}}(\varepsilon) = 1$. Alors son système naturel d'équations $[\mathbf{?}\Psi]^{\mathcal{S}}$ admet une solution naturelle unique dans la catégorie des ensembles.*

Démonstration. Rappelons que par le Lemme 5.4, pour tout $u \in \Psi$, $\textsc{Seq}_{\mathtt{L}}(u) = 1$ et $\textsc{Règ}(u) \in \mathfrak{R}$. On cherche donc à définir, pour chaque $u \in \Psi$, une transformation correspondante :

$$[u]^{\mathcal{S}}_{\Psi} : \prod_{v \in H_{\Psi}} \mathcal{E}\boldsymbol{ns}(\mathbf{1}, B^{\mathcal{S}}_v) \to \mathcal{E}\boldsymbol{ns}(\mathbf{1}, B^{\mathcal{S}}_u)\,,$$

où $B_v := [\![\textsc{Seq}_{\mathtt{R}}(v)]\!]_V$, de façon à ce que $[!\Psi]^{\mathcal{S}} = \langle [u]^{\mathcal{S}}_{\Psi}\rangle_{u\in\Psi}$ soit la solution recherchée. Or, puisqu'il y a, pour tout foncteur $F : \mathcal{Ens}^V \to \mathcal{Ens}$, un isomorphisme naturel :

$$\mathcal{Ens}(\mathbf{1}, F) \cong F\,,$$

alors le problème est équivalent à celui de définir

$$[u]^{\mathcal{S}}_{\Psi} : \prod_{v\in H_\Psi} B^{\mathcal{S}}_v \to B^{\mathcal{S}}_u\,.$$

On procède par induction sur $\mathcal{S}$. Si $\mathsf{BV}(\mathcal{S}) = \varnothing$, alors aucune règle de point fixe ne peut être appliquée dans Ψ. En particulier, il n'y a aucune branche infinie dans Ψ et, par le Lemme de Kőnig, Ψ est une preuve finie. On peut alors simplement se servir du Tableau 3.2 pour propager la solution des feuilles vers la racine. La solution ainsi obtenue est, par récurrence sur Ψ, la seule possible.

Si $\mathsf{BV}(\mathcal{S}) \neq \varnothing$, soit

$$M := \{u \in \Psi : \exists X \in \mathsf{MAX}(\mathcal{S}) \text{ t.q. } \textsc{Règ}(u) = \mathtt{RF}_X\}.$$

Pour tout $u \in M$ on dénotera par X_u la variable telle que $\textsc{Règ}(u) = \mathtt{RF}_{X_u}$.

Soit Ψ' la preuve obtenue de Ψ en justifiant chaque $u \in M$ par la règle d'hypothèse plutôt que par $\mathtt{RF}_{X_u}$ et en supprimant l'arête sortante de chacun. On dénote par $\widetilde{\mathcal{K}}$ l'ensemble des composantes connexes de Ψ', comme à la Section 1.5. Rappelons que chaque $K \in \widetilde{\mathcal{K}}$ est un arbre. Il a donc une racine qu'on dénote $\sqrt{K}$. Ainsi, chaque K est une preuve arborescente sur le système $\mathsf{P}(\mathcal{S})$. On définit une partition de H_K comme suit :

$$H^{\mathtt{M}}_K = H_K \cap M = K \cap M \qquad , \qquad H^{\mathtt{S}}_K = H_K \setminus M\,.$$

Par l'hypothèse d'induction, on peut résoudre le système $[?K]^{\mathsf{P}(\mathcal{S})}$. Chaque sommet $u \in K$ s'interprète alors comme une fonction :

$$[u]^{\mathsf{P}(\mathcal{S})}_K : \prod_{v\in H^{\mathtt{M}}_K} [\![X_v]\!]^{\mathsf{P}(\mathcal{S})}_V \times \prod_{v\in H^{\mathtt{S}}_K} B^{\mathsf{P}(\mathcal{S})}_v \to B^{\mathsf{P}(\mathcal{S})}_u\,.$$

De plus, $\forall u \in \Pi$, il existe clairement une unique composante $K_u \in \widetilde{\mathcal{K}}$ telle que $u \in K_u$.

Similairement à ce qu'on a fait au Théorème 4.4, on ordonne $\widetilde{\mathcal{K}}$ par la relation d'ordre $\leq$ duale à la relation $\sqsubseteq$ décrite à la Section 1.5. On a donc :

$$K \leq K' \quad \iff \quad \exists u \in K' \text{ et } \exists v \in K \text{ tels que } u \twoheadrightarrow_\Psi v\,.$$

Soit $m = p_{\mathsf{MAX}(\mathcal{S})}$. On argumente selon la parité de m.

Si m est impair (μ), alors la relation $\leq$ est bien fondée. En effet, supposons, au contraire, qu'il existe une chaîne infinie $K_0 > K_1 > K_2 > \cdots \in \widetilde{\mathcal{K}}$. Alors, pour tout $i \in \mathbb{N}$, il existe $u \in K_i$ et $v \in K_{i+1}$ tels que $u \twoheadrightarrow_\Psi v$. Or, puisque K_i et K_{i+1} sont des arbres, on a $\sqrt{K_i} \twoheadrightarrow_{K_i} u$ et $\sqrt{K_{i+1}} \twoheadrightarrow_{K_{i+1}} v$. Ainsi, par le Lemme 1.2, on a $u \twoheadrightarrow_\Psi \sqrt{K_{i+1}}$ ou $\sqrt{K_{i+1}} \twoheadrightarrow_\Psi u$. Cette seconde possibilité est disqualifiée puisqu'elle impliquerait $u \in K_{i+1}$. On a donc $\sqrt{K_i} \twoheadrightarrow_\psi \sqrt{K_{i+1}}$. Ainsi, on a trouvé un chemin infini dans Ψ :

$$\Gamma := \sqrt{K_0} \twoheadrightarrow_\Psi \sqrt{K_1} \twoheadrightarrow_\psi \sqrt{K_2} \twoheadrightarrow_\Psi \ldots.$$

Par la condition de garde, on a $\Gamma = \Gamma_0 \cdot \Gamma_1$ où Γ_1 a soit une μ-trace gauche ou une ν-trace droite. L'éventualité d'une μ-trace gauche est disqualifiée par le fait qu'aucune règle gauche n'est utilisée dans Ψ. Ainsi, Γ_1 a une ν-trace droite. Or, $\forall i > 0$, l'unique prédécesseur de $\sqrt{K_i}$ dans Ψ appartient à M. Il s'ensuit que Γ_1 visite une infinité de sommets u tels que $\text{RÈG}(u) = \mathtt{RF}_X$ et $X \in \mathsf{MAX}(\mathcal{S})$. Comme $\mathsf{MAX}(\mathcal{S})$ est fini, par le principe des nids de pigeons, $\exists X \in \mathsf{MAX}(\mathcal{S})$ tel que Γ_1 visite une infinité de sommets u tels que $\text{RÈG}(u) = \mathtt{RF}_X$. Puisque $X \in \mathsf{MAX}(\mathcal{S})$, c'est clairement l'une des variables les plus prioritaires visitées infiniment souvent par Γ_1. Or, puisque Γ_1 a une ν-trace droite, on conclut que $m = p_X$ est pair : une contradiction.

Puisque $\leq$ est bien fondée, on peut construire la solution $[!\Psi]^{\mathcal{S}}$ par induction sur $\widetilde{\mathcal{K}}$.

Soit $K \in \widetilde{\mathcal{K}}$ et $u \in K$. Si $u \in K \cap M$, alors $\mathrm{R\grave{E}G}(u) = \mathtt{RF}_{X_u}$ et $\varsigma u \in K' < K$. Par induction, la fonction

$$[\varsigma u]^{\mathcal{S}}_{\Psi} : \prod_{v \in H_\Psi} B^{\mathcal{S}}_v \to [\![F_{X_v}]\!]^{\mathcal{S}}$$

est bien définie. On pose alors simplement $[u]^{\mathcal{S}}_{\Psi} = [\varsigma u]^{\mathcal{S}}_{\Psi} \cdot \alpha_{X_u}$.

Supposons maintenant $u \in K \setminus M$. Pour tout $v \in \Psi$, rappelons qu'il existe, par le Lemme 2.8, un isomorphisme naturel

$$\eta_v \ : \ B^{\mathcal{S}}_v \to B^{\mathsf{P}(\mathcal{S})}_v(\vec{X}, \mathtt{id})\,,$$

où $\vec{X}$ est le foncteur $\langle [\![X]\!]^{\mathcal{S}}_V \rangle_{X \in \mathsf{MAX}(\mathcal{S})}$. Soit $\vec{f} = \langle [v]^{\mathcal{S}}_{\Psi} \rangle_{v \in H^{\mathtt{M}}_K}$ (c'est bien défini par le paragraphe précédent). Alors on définit $[u]^{\mathcal{S}}_{\Psi}$ par la composition suivante :

$$\begin{aligned}
\prod_{v \in H_\Psi} B^{\mathcal{S}}_v &\xrightarrow{\langle \vec{f}\,, \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K} \rangle} \prod_{v \in H^{\mathtt{M}}_K} [\![X_v]\!]^{\mathcal{S}} \times \prod_{v \in H^{\mathtt{S}}_K} B^{\mathcal{S}}_v \\
&\xrightarrow{\prod_{v \in H_K} \eta_v} \prod_{v \in H^{\mathtt{M}}_K} [\![X_v]\!]^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id}) \times \prod_{v \in H^{\mathtt{S}}_K} B^{\mathsf{P}(\mathcal{S})}_v(\vec{X}, \mathtt{id}) \\
&\xrightarrow{[u]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})}} B^{\mathsf{P}(\mathcal{S})}_u(\vec{X}, \mathtt{id}) \\
&\xrightarrow{\eta_u^{-1}} B^{\mathcal{S}}_u\,.
\end{aligned}$$

Il faut vérifier que notre définition est bien une solution à $[\mathtt{?}\Psi]^{\mathcal{S}}$. Cela est évident (par définition) si $u \in M$. Si $u \in K \setminus M$, soit

$$\delta = \langle \vec{f}\,, \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K} \rangle \cdot \big(\prod_{v \in H_K} \eta_v \big)\,.$$

Alors on a bien

$$\begin{aligned}
[u]^{\mathcal{S}}_{\Psi} &= \delta \cdot [u]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})} \cdot \eta_u^{-1} \\
&= \delta \cdot \big\langle [v]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})} \big\rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathsf{P}(\mathcal{S})}_{(\vec{X},\mathtt{id})} \cdot \eta_u^{-1} \\
&= \big\langle \delta \cdot [v]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})} \cdot \eta_v^{-1} \big\rangle_{v \in \mathrm{suc}(u)} \cdot \big(\eta_v\big)_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathsf{P}(\mathcal{S})}_{(\vec{X},\mathtt{id})} \cdot \eta_u^{-1} \\
&= \langle [v]^{\mathcal{S}}_K \rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathcal{S}}\,.
\end{aligned}$$

Si m est pair (ν), on procède plutôt de façon similaire à la Proposition 4.3. Pour tout $u \in C_\Psi$, soit $K \in \widetilde{\mathcal{K}}$ la composante contenant ςu et soit θ^u la transformation naturelle obtenue par la composition suivante :

$$\prod_{v\in M} [\![X_v]\!]^{\mathsf{P}(\mathcal{S})} \times \prod_{v\in H_\Psi} B_v^{\mathsf{P}(\mathcal{S})} \xrightarrow{\mathtt{pr}^{M}_{H^{\mathtt{M}}_K} \times \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K}} [\![X_v]\!]^{\mathsf{P}(\mathcal{S})} \times \prod_{v\in H^{\mathtt{S}}_K} B_v^{\mathsf{P}(\mathcal{S})} \xrightarrow{[\varsigma u]^{\mathsf{P}(\mathcal{S})}_K} [\![F_{X_u}]\!]^{\mathsf{P}(\mathcal{S})}.$$

Soit $\vartheta = \langle \theta^u \rangle_{u\in M}$. Il s'agit d'une transformation naturelle

$$\vartheta : \prod_{u\in M} [\![X_u]\!]^{\mathsf{P}(\mathcal{S})} \times \prod_{v\in H^{\mathtt{S}}_K} B_v^{\mathsf{P}(\mathcal{S})} \to \prod_{u\in M} [\![F_{X_u}]\!]^{\mathsf{P}(\mathcal{S})}.$$

Soit $W = \mathsf{MAX}(\mathcal{S})$. Pour tout $X \in W$, soit $M_X = \{u \in M : X_u = X\}$. On définit deux isomorphismes naturels comme suit :

$$\begin{aligned}
\sigma : \prod_{u\in M} [\![X_u]\!]^{\mathsf{P}(\mathcal{S})} &\xrightarrow{\sim} \prod_{X\in W} \prod_{u\in M_X} [\![X_u]\!]^{\mathsf{P}(\mathcal{S})} \\
&= \prod_{X\in W} \prod_{u\in M_X} [\![X]\!]^{\mathsf{P}(\mathcal{S})} \\
&\xrightarrow{\sim} \prod_{X\in W} \mathcal{E}\mathit{ns}\big(M_X\,,\, [\![X]\!]^{\mathsf{P}(\mathcal{S})}\big) \\
&= \prod_{X\in W} \mathcal{E}\mathit{ns}\big(M_X\,,\, \mathtt{pr}_X\big)
\end{aligned}$$

et, de façon similaire :

$$\begin{aligned}
\tau : \prod_{u\in M} [\![F_{X_u}]\!]^{\mathsf{P}(\mathcal{S})} &\xrightarrow{\sim} \prod_{X\in W} \prod_{u\in M_X} [\![F_{X_u}]\!]^{\mathsf{P}(\mathcal{S})} \\
&= \prod_{X\in W} \prod_{u\in M_X} [\![F_X]\!]^{\mathsf{P}(\mathcal{S})} \\
&\xrightarrow{\sim} \prod_{X\in W} \mathcal{E}\mathit{ns}\big(M_X\,,\, [\![F_{X_u}]\!]^{\mathsf{P}(\mathcal{S})}\big).
\end{aligned}$$

Soit $\vartheta' = (\sigma^{-1} \times \mathtt{id}) \cdot \vartheta \cdot \tau$. Alors $\vartheta'_{x,z}$ est du type suivant :

$$\prod_{X\in W} \mathcal{E}\mathit{ns}\big(M_X\,,\, \mathtt{pr}_X(x)\big) \times \prod_{v\in H_\Psi} B_v^{\mathsf{P}(\mathcal{S})}(x,z) \to \prod_{X\in W} \mathcal{E}\mathit{ns}\big(M_X\,,\, [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}(x,z)\big).$$

C'est donc une instance du Lemme 2.6, avec $I = W$, $\mathcal{C} = \mathcal{Ens}$, $\mathcal{Y} = \mathbb{1}$, $\mathcal{Z} = \mathcal{Ens}^V$ et $G = \big\langle [\![F_X]\!]^{\mathsf{P}(\mathcal{S})} \big\rangle_{X \in W}$. Notons que la coalgèbre finale paramétrique du foncteur G est la paire $(\vec{X}, \vec{\zeta})$, où $\vec{X} = \big\langle [\![X]\!]^{\mathcal{S}} \big\rangle_{X \in W}$ et $\vec{\zeta} = \prod_{X \in W} (\zeta_X \cdot \xi_X)$, où

$$\xi_X : [\![F_X]\!]^{\mathcal{S}} \to [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id})$$

est l'isomorphisme naturel donné par le Lemme 2.8. Ainsi, par le Lemme 2.6, il existe une unique transformation naturelle

$$g : \prod_{v \in H_\Psi} B_v^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id}) \to \prod_{X \in W} \mathcal{Ens}\big(M_X \,,\, [\![X]\!]^{\mathcal{S}}\big),$$

telle que, pour tout $z \in \mathcal{Ens}^V$ et $q \in \prod_{v \in H_\Psi} B_v^{\mathsf{P}(\mathcal{S})}(\vec{X}(z), z)$, on a

$$g_z(q) \cdot \vec{\zeta}_z = \vartheta'_{\vec{X}(z), z}(g_z(q), q)\,. \tag{6.1}$$

Or, rappelons qu'on a un isomorphisme naturel :

$$\delta = \sigma^{-1}_{\vec{X}, \mathtt{id}} : \prod_{X \in W} \mathcal{Ens}\big(M_X \,,\, [\![X]\!]^{\mathcal{S}}\big) \to \prod_{u \in M} [\![X_u]\!]^{\mathcal{S}}.$$

Ainsi, pour tout $u \in M$, on définit $h_u = g \cdot \delta \cdot \mathtt{pr}_u$. De façon similaire au cas où m était impair, on étend cette solution à Ψ de la façon suivante. Soit $u \in \Psi \setminus M$ et $K \in \widetilde{\mathcal{K}}$ tel que $u \in K$. Alors on définit h_u par la composition suivante :

$$\begin{aligned}
\prod_{v \in H_\Psi} B_v^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id}) &\xrightarrow{\langle g \cdot \delta \cdot \mathtt{pr}^{M}_{H^{\mathtt{M}}_K} \,,\, \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K} \rangle} \prod_{v \in H^{\mathtt{M}}_K} [\![X_v]\!]^{\mathcal{S}} \times \prod_{v \in H^{\mathtt{S}}_K} B_v^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id}) \\
&\xrightarrow{\quad = \quad} \prod_{v \in H^{\mathtt{M}}_K} [\![X_v]\!]^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id}) \times \prod_{v \in H^{\mathtt{S}}_K} B_v^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id}) \\
&\xrightarrow{[u]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X}, \mathtt{id})}} B_u^{\mathsf{P}(\mathcal{S})}(\vec{X}, \mathtt{id})\,.
\end{aligned}$$

Enfin, pour tout $u \in \Psi$, on pose $[u]^{\mathcal{S}}_\Psi = \big(\prod_{v \in H_\Psi} \eta_v\big) \cdot h_u \cdot \eta_u^{-1}$. On a donc

$$[u]^{\mathcal{S}}_\Psi : \prod_{v \in H_\Psi} B_v^{\mathcal{S}} \to B_u^{\mathcal{S}}\,.$$

Il ne reste qu'à vérifier qu'il s'agit d'une solution, c'est-à-dire que pour tout $u \in \Psi$, on a

$$[u]^{\mathcal{S}}_{\Psi} = \langle [v]^{\mathcal{S}}_{\Psi} \rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathcal{S}}.$$

Si $u \in \Psi \setminus M$, on peut le vérifier de façon similaire au cas de m impair. Soit $\vec{\eta} = \prod_{v \in H_\Psi} \eta_v$ et $\gamma = \vec{\eta} \cdot \langle g \cdot \delta \cdot \mathtt{pr}^{M}_{H^{\mathtt{M}}_K} , \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K} \rangle$. Alors on a :

$$\begin{aligned}
[u]^{\mathcal{S}}_{\Psi} &= \vec{\eta} \cdot h_u \cdot \eta_u^{-1} \\
&= \vec{\eta} \cdot \langle g \cdot \delta \cdot \mathtt{pr}^{M}_{H^{\mathtt{M}}_K} , \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K} \rangle \cdot [u]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})} \cdot \eta_u^{-1} \\
&= \gamma \cdot \big\langle [v]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})} \big\rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathsf{P}(\mathcal{S})}_{(\vec{X},\mathtt{id})} \cdot \eta_u^{-1} \\
&= \big\langle \gamma \cdot [v]^{\mathsf{P}(\mathcal{S})}_{K;(\vec{X},\mathtt{id})} \cdot \eta_v^{-1} \big\rangle_{v \in \mathrm{suc}(u)} \cdot \big(\eta_v\big)_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathsf{P}(\mathcal{S})}_{(\vec{X},\mathtt{id})} \cdot \eta_u^{-1} \\
&= \langle [v]^{\mathcal{S}}_{K} \rangle_{v \in \mathrm{suc}(u)} \cdot [\mathrm{R\grave{E}G}(u)]^{\mathcal{S}} .
\end{aligned}$$

Si $u \in M$, on effectue plutôt la vérification suivante. Soit $K \in \widetilde{\mathcal{K}}$ tel que $\varsigma u \in K$ et soit $\vec{\eta} = \big(\eta_v\big)_{v \in H_\Psi}$. Posons aussi $\vec{X}' = \big\langle [\![X_u]\!]^{\mathcal{S}} \big\rangle_{u \in M}$ et $\vec{\zeta}' = \prod_{u \in M} (\zeta_{X_u} \cdot \xi_{X_u})$ et

$$\varepsilon = \tau^{-1}_{\vec{X},\mathtt{id}} : \prod_{X \in W} \mathcal{E}\mathit{ns}\big(M_X , [\![F_X]\!]^{\mathsf{P}(\mathcal{S})}(\vec{X},\mathtt{id})\big) \to \prod_{u \in M} [\![F_{X_u}]\!]^{\mathsf{P}(\mathcal{S})}(\vec{X},\mathtt{id}).$$

Alors, clairement, on a $\delta \cdot \vec{\zeta}' = \vec{\zeta} \cdot \varepsilon$. Enfin, rappelons que, par le Lemme 2.8, on a $\eta_u = \mathtt{id}$. Alors :

$$\begin{aligned}
[u]^{\mathcal{S}}_{\Psi} &= \vec{\eta} \cdot h_u \cdot \eta_u^{-1} \\
&= \vec{\eta} \cdot g \cdot \delta \cdot \mathtt{pr}_u \\
&= \vartheta'_{\vec{X},\mathtt{id}}(\vec{\eta} \cdot g, \vec{\eta}) \cdot \vec{\zeta}^{-1} \cdot \delta \cdot \mathtt{pr}_u \\
&= \vartheta'_{\vec{X},\mathtt{id}}(\vec{\eta} \cdot g, \vec{\eta}) \cdot \varepsilon \cdot \vec{\zeta}'^{-1} \cdot \mathtt{pr}_u \\
&= \vartheta_{\vec{X},\mathtt{id}}(\vec{\eta} \cdot g \cdot \delta, \vec{\eta}) \cdot \varepsilon^{-1} \cdot \varepsilon \cdot \mathtt{pr}_u \cdot \xi^{-1}_{X_u} \cdot \zeta^{-1}_{X_u} \\
&= \theta^{u}_{\vec{X},\mathtt{id}}(\vec{\eta} \cdot g \cdot \delta, \vec{\eta}) \cdot \xi^{-1}_{X_u} \cdot \zeta^{-1}_{X_u} \\
&= \langle \vec{\eta} \cdot g \cdot \delta, \vec{\eta} \rangle \cdot (\mathtt{pr}^{M}_{H^{\mathtt{M}}_K} \times \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K}) \cdot [\varsigma u]^{\mathsf{P}(\mathcal{S})}_{K;\vec{X},\mathtt{id}} \cdot \xi^{-1}_{X_u} \cdot \zeta^{-1}_{X_u} \\
&= \vec{\eta} \cdot \langle g \cdot \delta \cdot \mathtt{pr}^{M}_{H^{\mathtt{M}}_K} , \mathtt{pr}^{H_\Psi}_{H^{\mathtt{S}}_K} \rangle \cdot [\varsigma u]^{\mathsf{P}(\mathcal{S})}_{K;\vec{X},\mathtt{id}} \cdot \eta^{-1}_{\varsigma u} \cdot \zeta^{-1}_{X_u} \\
&= [\varsigma u]^{\mathcal{S}}_{\Psi} \cdot [\mathtt{RF}_{X_u}]^{\mathcal{S}} .
\end{aligned}$$

Réciproquement, toute solution au système $[\mathbf{?}\Psi]^{\mathcal{S}}$ engendre une solution à l'équation (6.1) en remontant le calcul, d'où on conclut qu'il y a unicité. □

Comme corollaire de la proposition précédente, on a le théorème d'adéquation pour les preuves arborescentes.

Théorème 6.3 (Adéquation)**.** *Soit Ψ une preuve arborescente sans coupures sur un système $\mathcal{S}$ telle que $\textsc{Seq}_{\mathtt{L}}(\varepsilon) = 1$. Alors Ψ est résoluble dans la catégorie des ensembles.*

Démonstration. Par le Lemme 5.4, pour tout $u \in \Psi$, on a $\textsc{Règ}(u) \in \mathfrak{R} \cup \{\mathtt{I}\}$ et $\textsc{Seq}_{\mathtt{L}}(u) = 1$. On peut supposer, sans perte de généralité, qu'il n'y a aucune occurrence de la règle $\mathtt{I}$ dans Ψ. En effet, la règle $\mathtt{I}$ ne sert qu'à justifier le séquent $1 \vdash 1$. Soit donc $\Psi' = \langle \Psi, \textsc{Règ}', \textsc{Seq} \rangle$ la preuve arborescente obtenue en posant

$$\textsc{Règ}'(u) = \begin{cases} \mathtt{RAx} & \text{si } \textsc{Règ}(u) = \mathtt{I}\,; \\ \textsc{Règ}(u) & \text{sinon.} \end{cases}$$

Puisqu'il n'existe qu'une seule fonction $!_{\mathbf{1}} : \mathbf{1} \to \mathbf{1}$, alors Ψ et Ψ' ont le même système d'équations et, en particulier, Ψ est résoluble si et seulement si Ψ' l'est.

On cherche donc à définir, pour chaque $u \in \Psi$, une transformation correspondante :

$$[\![u]\!]_{\Psi} : \prod_{v \in H_{\Psi}} \mathcal{E}\mathit{ns}_V(\mathbf{1}, B_v) \to \mathcal{E}\mathit{ns}_V(\mathbf{1}, B_u)\,,$$

où $B_v := [\![\textsc{Seq}_{\mathtt{R}}(v)]\!]_V$, de façon à ce que $[\![\mathbf{!}\Psi]\!] = \langle [\![u]\!]_{\Psi} \rangle_{u \in \Psi}$ soit la solution recherchée. Or, ce problème est équivalent, à isomorphisme près, à celui de définir

$$[\![u]\!]_{\Psi} : \mathcal{E}\mathit{ns}_V\Big(\mathbf{1}, \prod_{v \in H_{\Psi}} B_v\Big) \to B_u\,.$$

Par la Proposition 6.2, le système naturel d'équations associé à Ψ admet une unique solution naturelle

$$[!\Psi] : \prod_{u \in H_\Psi} B_u \to \prod_{v \in C_\Psi} B_v \,.$$

Soit $x \in \mathcal{Ens}_V\Big(\mathbf{1}, \prod_{v \in H_\Psi} B_v\Big)$. Pour tout $u \in C_\Psi$, on pose $[\![u]\!]_\Psi(x) = (\gamma_c)_{c \in \mathcal{C}^V}$, où

$$\gamma_c := x_c \cdot [!\Psi]_{c,c} \cdot \mathtt{pr}_u^{C_\Psi} \,.$$

Par le Lemme 4.2, $[\![u]\!]_\Psi(x)$ est bel et bien une transformation naturelle

$$[\![u]\!]_\Psi(x) : \mathbf{1} \to B_u \,.$$

Enfin, comme au Théorème 4.4, on a

$$\begin{aligned}
\gamma_c &= x_c \cdot [!\Psi]_{c,c} \cdot \mathtt{pr}_u^{C_\Psi} \\
&= x_c \cdot \big([?\Psi]([!\Psi], \mathtt{id}) \big)_{c,c} \cdot \mathtt{pr}_u^{C_\Psi} \\
&= x_c \cdot [?\Psi]_{c,c}\big([!\Psi]_{c,c}, \mathtt{id}_{c,c} \big) \cdot \mathtt{pr}_u^{C_\Psi} \\
&= [\mathrm{R\grave{E}G}(u)]_{c,c} \circ \mathtt{pr}^{\Psi}_{\mathrm{suc}(u)}\big(x_c \cdot [!\Psi]_{c,c}, x_c \big) \\
&= [\![\mathrm{R\grave{E}G}(u)]\!]_c \circ \langle ([\![v]\!]_\Psi(x))_c \rangle_{v \in \mathrm{suc}(u)} \,.
\end{aligned}$$

On conclut donc $[\![u]\!]_\Psi = [\![\mathrm{R\grave{E}G}(u)]\!] \circ \langle [\![v]\!]_\Psi \rangle_{v \in \mathrm{suc}(u)}$. □

Soit Ψ comme dans le résultat précédent. On définit $[\![\Psi]\!] := [\![\varepsilon]\!]_\Psi$. On a également un théorème de plénitude pour les preuves arborescentes sans coupures.

Théorème 6.4 (Plénitude)**.** *Soit $\mathcal{S}$ un système dirigé d'équations et $\varphi \in \mathfrak{F}_V$, où $\mathsf{BV}(\mathcal{S}) \subseteq V$. Pour tout $x \in \mathcal{Ens}_V(\mathbf{1}, [\![\varphi]\!])$, il existe une preuve arborescente canonique Ψ_x sur $\mathcal{S}$, sans coupures ni identités, telle que $\textsc{Seq}(\varepsilon) = 1 \vdash \varphi$, et $[\![\Psi_x]\!] = x$. De plus, si $\mathcal{S}$ est clos et $\mathsf{VAR}(\varphi) \subseteq \mathsf{BV}(\mathcal{S})$, alors Ψ_x est une preuve close.*

Démonstration. Soit $x \in \mathcal{Ens}_V(\mathbf{1}, [\![\varphi]\!])$. On procède par induction sur φ.

– Si $\varphi = 0$, il n'y a rien à démontrer, puisqu'il n'existe aucune fonction $x : \mathbf{1} \to \mathbf{0}$ dans $\mathcal{Ens}$.

– Si $\varphi = 1$, on pose :

$$\Psi_x := \frac{}{1 \vdash 1}\,\mathtt{RAx}.$$

– Si $\varphi = X \in V \setminus \mathsf{BV}(\mathcal{S})$, on pose :

$$\Psi_x := \frac{}{1 \vdash X}\,\mathtt{H}.$$

– Si $\varphi = X \in \mathsf{BV}(\mathcal{S})$, soit $\theta = \alpha_X^{-1}$ si p_X est impair, et $\theta = \zeta_X$ si p_X est pair. On pose alors :

$$\Psi_x := \frac{\dfrac{}{1 \vdash F_X}\,\Psi_{x\cdot\theta}}{1 \vdash X}\,\mathtt{RF}_X.$$

– Si $\varphi = (\varphi_0 \times \varphi_1)$, on pose :

$$\Psi_x := \frac{\dfrac{}{1 \vdash \varphi_0}\,\Psi_{x\cdot\mathtt{pr}_0} \qquad \dfrac{}{1 \vdash \varphi_1}\,\Psi_{x\cdot\mathtt{pr}_1}}{1 \vdash \varphi_0 \times \varphi_1}\,\mathtt{R}\times \quad .$$

– Si $\varphi = (\varphi_0 + \varphi_1)$, montrons d'abord qu'il existe $j \in \{0,1\}$ et $y : \mathbf{1} \to [\![\varphi_j]\!]$ tels que $x = y \cdot \mathtt{in}_j$. En effet, rappelons que dans la catégorie des ensembles, le coproduit peut être défini par l'équation

$$A + B := \{\langle 0, a\rangle : a \in A\} \cup \{\langle 1, b\rangle : b \in B\}$$

et les injections sont définies par $\mathtt{in}_j(z) := \langle j, z\rangle$. Ainsi, $\forall a \in \mathcal{Ens}^V$, il existe $j_a \in \{0,1\}$ et $y_a \in [\![\varphi_{j_a}]\!](a)$ tels que $x_a = \langle j_a, y_a\rangle$. Par naturalité de x, $\forall f : a \to b$ dans $\mathcal{Ens}^V$, on a

$$\begin{aligned}
\langle j_b, y_b\rangle &= x_b \\
&= x_a \cdot ([\![\varphi_0]\!] + [\![\varphi_1]\!])(f) \\
&= \langle j_a, y_a\rangle \cdot ([\![\varphi_0]\!] + [\![\varphi_1]\!])(f) \\
&= \langle j_a, y_a \cdot [\![\varphi_{j_a}]\!](f)\,.
\end{aligned}$$

En particulier, $j_a = j_b =: j$ et $y_b = y_a \cdot [\![\varphi_{j_a}]\!](f)$. Ainsi, $y = (y_a)_{a \in \mathcal{E}ns^V}$ est une transformation naturelle $\mathbf{1} \to [\![\varphi_j]\!]$ telle que $x = y \cdot \mathtt{in}_j$. On pose alors :

$$\Psi_x := \dfrac{\dfrac{}{1 \vdash \varphi_j}\,\Psi_y}{1 \vdash \varphi_0 \times \varphi_1}\,\mathtt{R}{+_j}.$$

Par construction, il est immédiat que la pré-preuve Ψ_x est résoluble et $[\![\Psi_x]\!] = x$. De plus, aucun des cas dans la définition de Ψ_x n'utilise les règles `C` ou `I` et le seul cas où `H` est utilisé est pour justifier le séquent $1 \vdash X$ pour $X \in V \setminus \mathsf{BV}(\mathcal{S})$. Par récurrence, cette situation ne se produira jamais à condition d'avoir $\mathcal{S}$ clos et $\mathsf{VAR}(\varphi) \subseteq \mathsf{BV}(\mathcal{S})$.

Il ne reste donc qu'à démontrer que Ψ_x est une *preuve*, c'est-à-dire qu'elle satisfait la condition de garde. Or, cela est une conséquence du Théorème 2.10. En effet, les étapes de la construction ici proposée correspondent aux mouvements pour un des deux joueurs dans le jeu $J(\mathcal{S})$. Or, puisque x a comme valeur un élément de $[\![\varphi]\!](E)$ (pour tout E), alors la stratégie décrite par Ψ_x doit être gagnante pour σ. Or, cela est équivalent à affirmer que chaque chemin infini Γ de Ψ_x se décompose en $\Gamma = \Gamma_0 \cdot \Gamma_1$ où Γ_1 a une ν-trace droite. □

Proposition 6.5. *Soit Ψ_1, Ψ_2 deux preuves arborescentes closes, sans occurrences des règles `C` ni `I`, telles que le séquent à la racine est, pour toutes les deux, de la forme $1 \vdash \varphi$. Alors si $[\![\Psi_1]\!] = [\![\Psi_2]\!]$, on peut conclure $\Psi_1 = \Psi_2$.*

Démonstration. Étant donné deux preuves arborescentes sans identités ni coupures, $\Psi_1 = \langle G_1, \text{RÈG}_1, \text{SEQ}_1 \rangle$ et $\Psi_2 = \langle G_2, \text{RÈG}_2, \text{SEQ}_2 \rangle$, on définit la relation suivante :

$$\Psi_1 \approx \Psi_2 \quad \Leftrightarrow \quad [\![\Psi_1]\!] = [\![\Psi_2]\!] \text{ et } \exists \varphi \text{ t.q. } \text{SEQ}_1(\varepsilon) = \text{SEQ}_2(\varepsilon) = 1 \vdash \varphi$$

Par le principe de coinduction (Théorème 2.7), il suffit de montrer que la relation $\approx$ est une bisimulation. Puisque les preuves arborescentes sont des instances d'arbres

à branchements finis doublement étiquetés (par des règles et des séquents), alors, par l'Exemple 5 de la Section 2.3, il faut donc montrer que si $\Psi_1 \approx \Psi_2$, alors les propriétés suivantes sont satisfaites :

1. $\text{RÈG}_1(\varepsilon) = \text{RÈG}_2(\varepsilon)$,
2. La racine a le même nombre de sous-arbres dans Ψ_1 et Ψ_2,
3. Pour tout i, $\Psi_1/i \approx \Psi_2/i$, où Ψ_j/i est le i-ème sous-arbre de Ψ_j à la racine.

Remarquons d'abord que puisqu'il n'y a aucune occurrence de $\mathtt{C}$ et de $\mathtt{I}$, les seules règles qui peuvent justifier un séquent de la forme $1 \vdash \varphi$ sont dans $\mathfrak{R}$. De plus, les choix possibles dépendent complètement de la forme de la formule φ. Observons chaque cas.

– Si $\varphi = 1$: alors $\text{RÈG}_1(\varepsilon) = \text{RÈG}_2(\varepsilon) = \mathtt{RAx}$ et les racines des deux arbres n'ont donc aucun sous-arbre.

– Si $\varphi = X \in \mathsf{BV}(\mathcal{S})$: alors $\text{RÈG}_1(\varepsilon) = \text{RÈG}_2(\varepsilon) = \mathtt{RF}_X$. Dans ce cas, les deux racines n'ont qu'un seul sous-arbre, avec le même séquent à la racine puisque $\text{SEQ}_1(0) = \text{SEQ}_2(0) = 1 \vdash F_X$. Enfin, soit $f = [\![\Psi_1/0]\!]$ et $g = [\![\Psi_2/0]\!]$. Si p_X est pair, on a

$$\begin{array}{rrcll} & [\![\Psi_1]\!] & = & [\![\Psi_2]\!] & \\ \Rightarrow & f \cdot \alpha_X & = & g \cdot \alpha_X & \\ \Rightarrow & f & = & g & \text{(car } \alpha_X \text{ est inversible).} \end{array}$$

De même, si p_X est impair, on a

$$\begin{array}{rrcll} & [\![\Psi_1]\!] & = & [\![\Psi_2]\!] & \\ \Rightarrow & f \cdot \zeta_X^{-1} & = & g \cdot \zeta_X^{-1} & \\ \Rightarrow & f & = & g & \text{(car } \zeta_X^{-1} \text{ est inversible).} \end{array}$$

– Si $\varphi = \varphi_0 \times \varphi_1$: Alors $\text{RÈG}_1(\varepsilon) = \text{RÈG}_2(\varepsilon) = \mathtt{R}\times$. Dans ce cas, les racines ont chacune deux sous-arbres, avec les même séquent à la racine puisque pour $i \in \{0,1\}$, $\text{SEQ}_1(i) = \text{SEQ}_2(i) = 1 \vdash B_i$. Enfin, pour $i \in \{0,1\}$, soit $f_i = [\![\Psi_1/i]\!]$

et $g_i = [\![\Psi_2/i]\!]$. On a donc

$$\begin{array}{rrcl} & [\![\Psi_1]\!] & = & [\![\Psi_2]\!] \\ \Rightarrow & \langle f_0, f_1\rangle & = & \langle g_0, g_1\rangle \\ \Rightarrow & \langle f_0, f_1\rangle \cdot \mathtt{pr}_i & = & \langle g_0, g_1\rangle \cdot \mathtt{pr}_i \\ \Rightarrow & f_i & = & g_i \end{array}$$

– Si $\varphi = \varphi_0 + \varphi_1$: Alors $\text{RÈG}_1(\varepsilon) = \mathtt{R}+_i$ et $\text{RÈG}_2(\varepsilon) = \mathtt{R}+_j$, pour certains $i, j \in \{0, 1\}$. Dans ce cas, les racines ont chacune un seul sous-arbre. Soit $f = [\![\Psi_1/0]\!]$ et $g = [\![\Psi_2/0]\!]$. On a donc

$$\begin{array}{rrcl} & [\![\Psi_1]\!] & = & [\![\Psi_2]\!] \\ \Rightarrow & f \cdot \mathtt{in}_i & = & g \cdot \mathtt{in}_j \\ \Rightarrow & \langle i, f\rangle & = & \langle j, g\rangle \end{array}$$

On peut donc conclure $i = j$ et $f = g$. La première de ces conclusions établit au passage $\text{RÈG}_1(\varepsilon) = \text{RÈG}_2(\varepsilon)$ et $\text{SEQ}_1(\varsigma\varepsilon) = \text{SEQ}_2(\varsigma\varepsilon) = 1 \vdash \varphi_i$. □

On veut généraliser le théorème d'élimination des coupures du Chapitre 5, qui concernait seulement les preuves circulaires, au cas des preuves arborescentes. Cela se fait sans trop de difficultés puisque le seul endroit, dans le Chapitre 5, où on exploite le fait que Π est une preuve circulaire est dans la démonstration du Lemme 5.25. Et encore là, ce n'est pas la finitude de Π qui est exploitée ni l'énoncé même de la condition de garde, mais seulement le fait qu'elle satisfait le Lemme 3.2. Or, ce Lemme signifie seulement que les preuves circulaires satisfont aussi la condition de garde des preuves arborescentes ! Ainsi, en calquant tout le Chapitre 5, on peut adapter tous ses résultats aux preuves arborescentes et définir $\text{CE}_\Psi(M)$, pour $M \in \mathcal{M}_\Psi$.

6.2 Sémantique de l'élimination des coupures

Fixons, pour cette section, une pré-preuve Π résoluble (pas nécessairement finie ou acyclique ou avec une forme particulière pour l'un de ses séquents) et telle que la définition de $\textsc{ce}_\Pi(M)$ de la Section 5.2 est productive, c'est-à-dire qu'il n'existe aucune $\bowtie$-chaîne infinie dans $\mathcal{M}_\Pi$. On cherche à démontrer explicitement que pour tout $r \in \Pi$, le système d'équations associé à $\textsc{ce}_\Pi(r)$ admet, à son tour, au moins une solution.

Définition. Soit $M = [u_1, u_2 \dots u_m]$ une multicoupure sur Π. La *sémantique* de M est définie comme suit :

$$[\![M]\!] := [\![u_1]\!]_\Pi \cdot [\![u_2]\!]_\Pi \cdots [\![u_m]\!]_\Pi.$$

Lemme 6.6. *Soit $M, N \in \mathcal{M}_\Pi$. Si $M \bowtie N$, alors $[\![M]\!] = [\![N]\!]$.*

Démonstration. Il suffit de vérifier que chaque opération interne sur une multicoupure préserve la sémantique de celle-ci. On vérifie chaque cas schématiquement, en évacuant l'utilisation des crochets sémantiques $[\![-]\!]$ pour des questions de lisibilité. Il s'agit donc de vérifier que dans chacune des figures suivantes, la sémantique de la racine du morceau de preuve présenté est préservée par l'opération.

• **Élimination des identités.**

$$\dfrac{A_0 \overset{f}{\cdots} \to B \quad \dfrac{}{B \xrightarrow{\mathtt{id}_B} B}\,\mathtt{I} \quad B \overset{g}{\cdots} \to A_m}{A_0 \xrightarrow{f \cdot \mathtt{id}_B \cdot g} A_m}\,\mathtt{C} \quad \overset{\textsc{IdÉlim}}{\Longrightarrow} \quad \dfrac{A_0 \overset{f}{\cdots} \to B \quad B \overset{g}{\cdots} \to A_m}{A_0 \xrightarrow{f \cdot g} A_m}\,\mathtt{C}$$

• **Fusion de coupures.**

$$\dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_i \qquad A_i \xrightarrow{a\cdot b} A_{i+1} \qquad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot(a\cdot b)\cdot g} A_m}\,\mathtt{C} \qquad \dfrac{A_i \xrightarrow{a} B \quad B \xrightarrow{b} A_{i+1}}{A_i \xrightarrow{a\cdot b} A_{i+1}}\,\mathtt{C}}{A_0 \xrightarrow{f\cdot(a\cdot b)\cdot g} A_m}$$

$$\Downarrow_{\textsc{Fusion}}$$

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_i \quad A_i \xrightarrow{a} B \quad B \xrightarrow{b} A_{i+1} \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot b\cdot g} A_m}\,\mathtt{C}$$

• **Réductions essentielles.**

– Si $\textsc{Règ}(u_i) = \mathtt{R}\times$ et $\textsc{Règ}(u_{i+1}) = \mathtt{L}\times_j$, pour $j \in \{0,1\}$:

$$\dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \qquad A_{i-1} \xrightarrow{\langle a,b\rangle} B_0 \times B_1 \qquad B_0 \times B_1 \xrightarrow{\mathtt{pr}_k\cdot c} A_{i+1} \qquad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot\langle a,b\rangle\cdot\mathtt{pr}_k\cdot c\cdot g} A_m}\,\mathtt{C} \qquad \dfrac{A_{i-1} \xrightarrow{a} B_0 \quad A_{i-1} \xrightarrow{b} B_1}{A_{i-1} \xrightarrow{\langle a,b\rangle} B_0 \times B_1}\,\mathtt{R}\times \qquad \dfrac{B_j \xrightarrow{c} A_{i+1}}{B_0 \times B_1 \xrightarrow{\mathtt{pr}_k\cdot c} A_{i+1}}\,\mathtt{L}\times_j}{A_0 \xrightarrow{f\cdot\langle a,b\rangle\cdot\mathtt{pr}_k\cdot c\cdot g} A_m}$$

$$\Downarrow_{\textsc{Réduct}}$$

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \quad A_{i-1} \xrightarrow{h_j} B_k \quad B_j \xrightarrow{c} A_{i+1} \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot h_j\cdot c\cdot g} A_m}\,\mathtt{C}$$

Dans le schéma ci-dessus, on a posé $h_j = a$ si $j = 0$ et $h_j = b$ si $j = 1$. Autrement dit, $h_j = \langle a, b\rangle \cdot \mathtt{pr}_j$ et on a l'égalité recherchée.

– Si $\textsc{Règ}(u_i) = \mathtt{R}+_j$ et $\textsc{Règ}(u_{i+1}) = \mathtt{L}+$, pour $j \in \{0,1\}$:

$$\dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \qquad A_{i-1} \xrightarrow{a\cdot\mathtt{in}_j} B_0 + B_1 \qquad B_0 + B_1 \xrightarrow{\{b,c\}} A_{i+1} \qquad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot\mathtt{in}_j\cdot\{b,c\}\cdot g} A_m}\,\mathtt{C} \qquad \dfrac{A_{i-1} \xrightarrow{a} B_j}{A_{i-1} \xrightarrow{a\cdot\mathtt{in}_j} B_0 + B_1}\,\mathtt{R}+_j \qquad \dfrac{B_0 \xrightarrow{b} A_{i+1} \quad B_1 \xrightarrow{c} A_{i+1}}{B_0 + B_1 \xrightarrow{\{b,c\}} A_{i+1}}\,\mathtt{L}+}{A_0 \xrightarrow{f\cdot a\cdot\mathtt{in}_j\cdot\{b,c\}\cdot g} A_m}$$

$$\Downarrow_{\textsc{Réduct}}$$

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \quad A_{i-1} \xrightarrow{a} B_j \quad B_j \xrightarrow{h_j} A_{i+1} \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot h_j\cdot g} A_m}\,\mathtt{C}$$

Dans le schéma ci-dessus, on a cette fois $h_j = b$ si $j = 0$ et $h_j = c$ si $j = 1$. Autrement dit, $h_j = \mathtt{in}_j \cdot \{b, c\}$ et on a l'égalité recherchée.

– Si $\text{RÈG}(u_i) = \texttt{RF}_X$, $\text{RÈG}(u_{i+1}) = \texttt{LF}_X$ et p_X est impair (μ) :

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \quad \dfrac{A_{i-1} \xrightarrow{a} F_X}{A_{i-1} \xrightarrow{a\cdot\alpha_X} X}\,\texttt{RF}_X \quad \dfrac{F_X \xrightarrow{b} A_{i+1}}{X \xrightarrow{\alpha_X^{-1}\cdot b} A_{i+1}}\,\texttt{LF}_X \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot\alpha_X\cdot\alpha_X^{-1}\cdot b\cdot g} A_m}\,\texttt{C}$$

$$\Downarrow_{\text{RÉDUCT}}$$

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \quad A_{i-1} \xrightarrow{a} F_X \quad F_X \xrightarrow{b} A_{i+1} \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot b\cdot g} A_m}\,\texttt{C}$$

– Si $\text{RÈG}(u_i) = \texttt{RF}_x$, $\text{RÈG}(u_{i+1}) = \texttt{LF}_x$ et p_X est pair (ν) :

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \quad \dfrac{A_{i-1} \xrightarrow{a} F_X}{A_{i-1} \xrightarrow{a\cdot\zeta_X^{-1}} X}\,\texttt{RF}_X \quad \dfrac{F_X \xrightarrow{b} A_{i+1}}{X \xrightarrow{\zeta_X\cdot b} A_{i+1}}\,\texttt{LF}_X \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot\zeta_X^{-1}\cdot\zeta_X\cdot b\cdot g} A_m}\,\texttt{C}$$

$$\Downarrow_{\text{RÉDUCT}}$$

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{i-1} \quad A_{i-1} \xrightarrow{a} F_X \quad F_X \xrightarrow{b} A_{i+1} \quad A_{i+1} \overset{g}{\cdots\!\to} A_m}{A_0 \xrightarrow{f\cdot a\cdot b\cdot g} A_m}\,\texttt{C}$$

□

Fixons une racine $r \in \Pi$. Chaque $u \in \text{CE}_\Pi(r)$ y a été ajouté via une production gauche ou droite à partir d'une multicoupure M. On pose alors $[\![u]\!]^? := [\![M]\!]$.

Proposition 6.7. $[\![-]\!]^?$ *est une solution au système d'équations associé à* $\text{CE}_\Pi(r)$.

Démonstration. Il suffit de comparer la sémantique d'une multicoupure M avant production, avec celle de ses successeurs immédiatement après production. En effet, par le Lemme 6.6, la sémantique de ces derniers demeurera inchangée jusqu'à-ce qu'ils donnent eux-mêmes lieu à des productions. Comme précédemment, on effectue ces vérifications schématiquement.

• **Productions gauches.**

– Si $\text{RÈG}(u_0) = \texttt{LAx}$:

$$\dfrac{\dfrac{}{\mathbf{0} \xrightarrow{?_{A_1}} A_1}\,\texttt{LAx} \qquad A_1 \overset{f}{\cdots} \to A_m}{\mathbf{0} \xrightarrow{?_{A_1} \cdot f} A_m}\,\texttt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{}{\mathbf{0} \xrightarrow{?_{A_m}} A_m}\,\texttt{LAx}$$

Puisque 0 est l'objet initial, il existe *une seule* flèche de $\mathbf{0}$ vers A_m. En particulier, on a $?_{A_1} \cdot f = ?_{A_m}$.

– Si $\text{RÈG}(u_0) = \texttt{L}\times_j$ pour $j \in \{0, 1\}$:

$$\dfrac{\dfrac{B_j \xrightarrow{a} A_1}{B_0 \times B_1 \xrightarrow{\texttt{pr}_j \cdot a} A_1}\,\texttt{L}\times_j \qquad A_1 \overset{f}{\cdots} \to A_m}{B_0 \times B_1 \xrightarrow{\texttt{pr}_j \cdot a \cdot f} A_m}\,\texttt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{B_j \xrightarrow{a} A_1 \quad A_1 \overset{f}{\cdots} \to A_m}{B_j \xrightarrow{a \cdot f} A_m}\,\texttt{C}\;\dfrac{}{B_0 \times B_1 \xrightarrow{\texttt{pr}_j \cdot a \cdot f} A_m}\,\texttt{L}\times_j$$

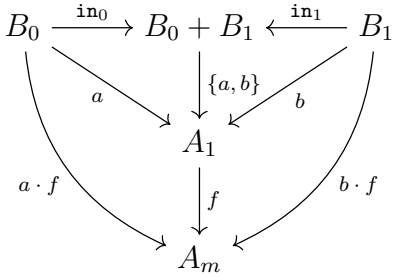
– Si $\text{RÈG}(u_0) = \texttt{L}+$:

$$\dfrac{\dfrac{B_0 \xrightarrow{a} A_1 \quad B_1 \xrightarrow{b} A_1}{B_0 + B_1 \xrightarrow{\{a,b\}} A_1}\,\texttt{L}+ \qquad A_1 \overset{f}{\cdots} \to A_m}{B_0 + B_1 \xrightarrow{\{a,b\} \cdot f} A_m}\,\texttt{C}$$

$$\Downarrow_{\text{LNEXT}}$$

$$\dfrac{\dfrac{B_0 \xrightarrow{a} A_1 \quad A_1 \overset{f}{\cdots} \to A_m}{B_0 \xrightarrow{a \cdot f} A_m}\,\texttt{C} \qquad \dfrac{B_1 \xrightarrow{b} A_1 \quad A_1 \overset{f}{\cdots} \to A_m}{B_1 \xrightarrow{a \cdot f} A_m}\,\texttt{C}}{B_0 + B_1 \xrightarrow{\{a \cdot f, b \cdot f\}} A_m}\,\texttt{L}+$$

L'égalité entre $\{a, b\} \cdot f$ et $\{a \cdot f, b \cdot f\}$ provient simplement de la propriété universelle du coproduit, puisque le diagramme suivant commute.



– Si $\text{RÈG}(u_0) = \mathtt{LF}_X$ et p_X est impair (μ) :

$$\dfrac{\dfrac{F_X \xrightarrow{a} A_1}{X \xrightarrow{\alpha_X^{-1}\cdot a} A_1}\,\mathtt{LF}_X \qquad A_1 \overset{f}{\cdots\!\to} A_m}{X \xrightarrow{\alpha_X^{-1}\cdot a\cdot f} A_m}\,\mathtt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{F_X \xrightarrow{a} A_1 \quad A_1 \overset{f}{\cdots\!\to} A_m}{\dfrac{F_X \xrightarrow{a\cdot f} A_m}{X \xrightarrow{\alpha_X^{-1}\cdot a\cdot f} A_m}\,\mathtt{LF}_X}\,\mathtt{C}$$

– Si $\text{RÈG}(u_0) = \mathtt{LF}_X$ et p_X est pair (ν) :

$$\dfrac{\dfrac{F_X \xrightarrow{a} A_1}{X \xrightarrow{\zeta_X\cdot a} A_1}\,\mathtt{LF}_X \qquad A_1 \overset{f}{\cdots\!\to} A_m}{X \xrightarrow{\zeta_X\cdot a\cdot f} A_m}\,\mathtt{C} \quad \overset{\text{LNEXT}}{\Longrightarrow} \quad \dfrac{F_X \xrightarrow{a} A_1 \quad A_1 \overset{f}{\cdots\!\to} A_m}{\dfrac{F_X \xrightarrow{a\cdot f} A_m}{X \xrightarrow{\zeta_X\cdot a\cdot f} A_m}\,\mathtt{LF}_X}\,\mathtt{C}$$

• Productions droites.

Le cas des productions droites suit du cas gauche par symétrie. Or, par souci de complétude, voici les vérifications au cas par cas.

– Si $\text{RÈG}(u_n) = \mathtt{RAx}$:

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \qquad \dfrac{}{A_{m-1} \xrightarrow{!_{A_{m-1}}} \mathbf{1}}\,\mathtt{RAx}}{A_0 \xrightarrow{f\cdot !_{A_{m-1}}} \mathbf{1}}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \dfrac{}{A_0 \xrightarrow{!_{A_0}} \mathbf{1}}\,\mathtt{RAx}$$

Puisque $\mathbf{1}$ est l'objet terminal, il existe *une seule* flèche de A_0 vers $\mathbf{1}$. En particulier, on a $f\cdot !_{A_{m-1}} = !_{A_0}$.

– Si $\text{RÈG}(u_n) = \mathtt{R}{+}_j$ pour $j \in \{0, 1\}$:

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \qquad \dfrac{A_{m-1} \xrightarrow{a} B_j}{A_{m-1} \xrightarrow{a\cdot \mathtt{in}_j} B_0 + B_1}\,\mathtt{R}{+}_j}{A_0 \xrightarrow{f\cdot a\cdot \mathtt{in}_j} B_0 + B_1}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \quad A_{m-1} \xrightarrow{a} B_j}{\dfrac{A_0 \xrightarrow{f\cdot a} B_j}{A_0 \xrightarrow{f\cdot a\cdot \mathtt{in}_j} B_0 + B_1}\,\mathtt{R}{+}_j}\,\mathtt{C}$$

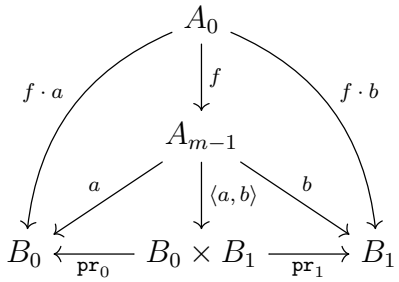
– Si $\text{RÈG}(u_n) = \mathtt{R}\times$:

$$\dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \qquad A_{m-1} \xrightarrow{\langle a,b\rangle} B_0 \times B_1}{A_0 \xrightarrow{f\cdot\langle a,b\rangle} B_0 \times B_1}\,\mathtt{C} \qquad \dfrac{A_{m-1} \xrightarrow{a} B_0 \quad A_{m-1} \xrightarrow{b} B_1}{A_{m-1} \xrightarrow{\langle a,b\rangle} B_0 \times B_1}\,\mathtt{R}\times}{A_0 \xrightarrow{f\cdot\langle a,b\rangle} B_0 \times B_1}\,\mathtt{C}$$

$$\Downarrow_{\text{RNEXT}}$$

$$\dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \quad A_{m-1} \xrightarrow{a} B_0}{A_0 \xrightarrow{f\cdot a} B_0}\,\mathtt{C} \qquad \dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \quad A_{m-1} \xrightarrow{b} B_1}{A_0 \xrightarrow{f\cdot b} B_1}\,\mathtt{C}}{A_0 \xrightarrow{\langle f\cdot a, f\cdot b\rangle} B_0 \times B_1}\,\mathtt{L}+$$

L'égalité entre $f \cdot \langle a, b\rangle$ et $\langle f \cdot a, f \cdot b\rangle$ provient simplement de la propriété universelle du produit, puisque le diagramme suivant commute.



– Si $\text{RÈG}(u_n) = \mathtt{RF}_X$ et p_X est impair (μ) :

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \qquad \dfrac{A_{m-1} \xrightarrow{a} F_X}{A_{m-1} \xrightarrow{a\cdot\alpha_X} X}\,\mathtt{RF}_X}{A_0 \xrightarrow{f\cdot a\cdot\alpha_X} X}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \quad A_{m-1} \xrightarrow{a} F_X}{A_0 \xrightarrow{f\cdot a} F_X}\,\mathtt{C}}{A_0 \xrightarrow{f\cdot a\cdot\alpha_X} X}\,\mathtt{RF}_X$$

– Si $\text{RÈG}(u_n) = \mathtt{RF}_X$ et p_X est pair (ν) :

$$\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \qquad \dfrac{A_{m-1} \xrightarrow{a} F_X}{A_{m-1} \xrightarrow{a\cdot\zeta_X^{-1}} X}\,\mathtt{RF}_X}{A_0 \xrightarrow{f\cdot a\cdot\zeta_X^{-1}} X}\,\mathtt{C} \quad \overset{\text{RNEXT}}{\Longrightarrow} \quad \dfrac{\dfrac{A_0 \overset{f}{\cdots\!\to} A_{m-1} \quad A_{m-1} \xrightarrow{a} F_X}{A_0 \xrightarrow{f\cdot a} F_X}\,\mathtt{C}}{A_0 \xrightarrow{f\cdot a\cdot\zeta_X^{-1}} X}\,\mathtt{RF}_X$$

□

Dans le cas où $\textsc{Seq}(r) = 1 \vdash \varphi$, on n'a, en apparence, rien appris de la présente section, car on savait depuis le Théorème 6.3 que $\textsc{ce}_\Pi(r)$ serait résoluble. On est toutefois parvenu, ici, à calculer cette solution, dont on enregistre la valeur à la racine dans le Lemme suivant :

Lemme 6.8. *Si* $\textsc{Seq}(r) = 1 \vdash \varphi$ *pour une formule* φ*, alors* $[\![\textsc{ce}_\Pi(r)]\!] = [\![r]\!]_\Pi$.

Démonstration. Soit M la multicoupure à un seul sommet $M := [r]$. Soit $N \in \mathcal{M}_\Pi$ un maximum local ($\nexists N'$ t.q. $N \bowtie N'$) tel que $M \overset{*}{\bowtie} N$. Alors

$$\begin{aligned}
[\![r]\!]_\Pi &= [\![M]\!] && \text{(par définition)}\\
&= [\![N]\!] && \text{(Lemme 6.6 appliqué plusieurs fois)}\\
&= [\![\textsc{ce}_\Pi(r)]\!]^? && \text{(par définition)}\\
&= [\![\textsc{ce}_\Pi(r)]\!]. && \text{(Théorème 6.3 et Proposition 6.7)} \quad \square
\end{aligned}$$

Lemme 6.9. *Soit* $M = [u_1 \dots u_m]$ *et* $N = [v_1 \dots v_n]$ *deux multicoupures telles que* $\textsc{Seq}_{\mathtt{L}}(u_1) = \textsc{Seq}_{\mathtt{L}}(v_1) = 1$ *et* $[\![M]\!] = [\![N]\!]$*. Supposons qu'il existe* $M', U, U' \in \mathcal{M}_\Pi$ *tels que* $M \cdot U \overset{*}{\bowtie} M' \cdot U'$*. Alors il existe* $N' \in \mathcal{M}_\Pi$ *tel que* $N \cdot U \overset{*}{\bowtie} N' \cdot U'$*.*

Démonstration. Il suffit de démontrer le cas où $M \cdot U \bowtie M' \cdot U'$: le cas général en découle par transitivité. Il y a trois situations à considérer.

1. $M = M'$ et $U \bowtie U'$: dans ce cas, on prend $N' = N$. En effet, $N \cdot U \bowtie N \cdot U'$ par le Lemme 5.3.
2. $M \bowtie M'$ et $U = U'$: dans ce cas, on prend encore $N' = N$. En effet, $N \cdot U \overset{*}{\bowtie} N \cdot U$ parce que $\overset{*}{\bowtie}$ est réflexive, par définition.
3. Sinon, $M \neq M'$ et $U \neq U'$. Soit $U = [w_1 \dots w_k]$. Alors

$$M \cdot U = [u_1 \dots u_{m-1}, u_m, w_1, w_2 \dots w_k].$$

La seule opération interne qui peut modifier à la fois l'un des u_i et l'un des w_j est $\textsc{Réduct}(M \cdot U, m)$. On a donc $\textsc{Règ}(u_m) \in \mathfrak{R}$, $\textsc{Règ}(w_1) \in \mathfrak{L}$ et

$$M' \cdot U' = [u_1 \dots u_{m-1}, u'_m, w'_1, w_2 \dots w_k]$$

où u'_m et w'_1 sont des successeurs de u_m et w_1 respectivement. Soit r la racine de $\textsc{ce}_\Pi(M)$. Puisque $\textsc{Règ}(u_m) \in \mathfrak{R}$, alors $\textsc{Seq}(r) = 1 \vdash \textsc{Seq}_{\mathtt{R}}(u_m)$ et $\textsc{Règ}(r) = \textsc{Règ}(u_m)$.

Puisque $\textsc{Seq}_{\mathtt{L}}(u_1) = \textsc{Seq}_{\mathtt{L}}(v_1) = 1$ et $[\![M]\!] = [\![N]\!]$, il s'ensuit, par la Proposition Lemme 6.5, que $\textsc{ce}_\Pi(M) = \textsc{ce}_\Pi(N)$. En particulier, leurs racines sont identiques. Soit $\widetilde{N} = [\widetilde{v}_1 \dots \widetilde{v}_\ell]$ une multicoupure maximale telle que $N \overset{*}{\nsim} \widetilde{N}$. C'est-à-dire que la racine de $\textsc{ce}_\Pi(N)$ est produite à partir de $\widetilde{N}$. On a donc $\textsc{Seq}_{\mathtt{R}}(\widetilde{v}_\ell) = \textsc{Seq}_{\mathtt{R}}(u_m)$ et $\textsc{Règ}(\widetilde{v}_\ell) = \textsc{Règ}(u_m)$. Or, notons que

$$\textsc{Réduct}(\widetilde{N} \cdot U, \ell) = [\widetilde{v}_1 \dots \widetilde{v}_{\ell-1}, \widetilde{v}'_\ell, w'_1, w_2 \dots w_k] = N' \cdot U'$$

où $\widetilde{v}'_\ell$ est un successeur de $\widetilde{v}_\ell$ et $N' = [\widetilde{v}_1 \dots \widetilde{v}_{\ell-1}, \widetilde{v}'_\ell]$. À l'aide du Lemme 5.3, on conclut que $N \cdot U \overset{*}{\nsim} \widetilde{N} \cdot U \nsim N' \cdot U'$. □

6.3 Concordance avec la sémantique dénotationnelle

Revenons à l'affirmation formulée en introduction de cette section, à l'effet que l'élimination des coupures peut servir à *calculer* les fonctions qu'on peut dénoter par des preuves circulaires.

Soit $A, B \in \mathfrak{F}$ et $\mathcal{S}$ un système dirigé d'équations. Soit aussi Π une preuve circulaire sur $\mathcal{S}$ dont on choisit une racine r telle que $\textsc{Seq}r = A \vdash B$. Par le Théorème 4.4, r dénote une transformation naturelle $f = [\![r]\!]_\Pi : [\![A]\!]^{\mathcal{S}} \to [\![B]\!]^{\mathcal{S}}$. C'est cette fonction qu'on cherche à calculer.

Or, pour tout $x : \mathbf{1} \to [\![A]\!]^{\mathcal{S}}$, rappelons qu'on peut, grâce au Théorème 6.4, lui associer, de façon canonique, une preuve arborescente sans coupure Ψ_x. Considérons

la pré-preuve $\Psi_x \odot \Pi$ suivante :

$$\dfrac{\dfrac{}{1 \vdash X}\,\Psi_x \qquad \dfrac{}{X \vdash Y}\,\Pi}{1 \vdash Y}\,\mathtt{C}$$

Il s'agit d'une pré-preuve possiblement infinie, avec au moins une coupure et possiblement des cycles. Soit z la racine de $\Psi_x \odot \Pi$. La solution de l'équation associée à z est facile à établir puisqu'on connaît la solution aux deux antécédants à la coupure. On a donc :

$$[\![z]\!]_{\Psi_x \odot \Pi} = [\![\varepsilon]\!]_{\Psi_x} \cdot [\![r]\!]_{\Pi} = x \cdot f = f(x).$$

On sait donc que $\Psi_x \odot \Pi$ est résoluble.

Après élimination des coupures dans $\Psi_x \odot \Pi$, on obtiendra donc une preuve sans coupure dont le séquent à la racine est $1 \vdash Y$. De dire que l'élimination des coupures *calcule* $f(x)$, c'est donc de dire que la preuve résultante n'est nulle autre que $\Psi_{f(x)}$ elle-même. C'est le résultat principal de cette section.

Théorème 6.10. $\mathrm{CE}_{\Psi_x \odot \Pi}(z) = \Psi_{f(x)}$.

Démonstration. $\mathrm{CE}_{\Psi_x \odot \Pi}(z)$ est une preuve arborescente sans coupure dont, le séquent à la racine est $1 \vdash Y$.

De plus, cette preuve ne contient pas d'occurrences de la règle `I`. En effet, pour qu'une telle occurrence surgisse de l'élimination des coupures, il faudrait qu'à une étape, la mémoire de l'éliminateur de coupures soit de la forme $M = [u]$ où $u \in \Psi_x \odot \Pi$ et $\mathrm{RÈG}(u) = \mathtt{I}$. Ce n'est pas à la première étape qu'une telle situation peut se produire, car $\mathrm{RÈG}(z) = \mathtt{C} \neq \mathtt{I}$. Par la suite, on peut voir par une simple récurrence que le sommet le plus à gauche dans M fait toujours partie de Ψ_x, qui ne contient pas d'occurrences de la règle `I`. De plus, par le Lemme 6.8, on a

$$[\![\mathrm{CE}_{\Psi_x \odot \Pi}(z)]\!] = [\![z]\!]_{\Psi_x \odot \Pi} = f(x) = [\![\Psi_{f(x)}]\!] .$$

La conclusion suit donc directement du Lemme 6.5. □

Troisième partie

Puissance expressive

CHAPITRE VII

ARBRES D'ORDRE SUPÉRIEUR

Au Chapitre 6, on a démontré que l'éliminateur de coupures était un modèle de machine abstraite pouvant calculer les fonctions qu'on peut dénoter par des preuves circulaires. Mais quelles sont ces fonctions, exactement ? C'est une question qui fut soulevée et partiellement répondue, dans le cas des fonctions numériques $f : \mathbb{N}^k \to \mathbb{N}$, dans (Paré et Román, 1989; Cockett et Santocanale, 2003), où il fut démontré que les fonctions primitives récursives en faisaient partie.

On a expliqué, au Chapitre 5, que l'éliminateur de coupures était une sorte d'automate fini avec mémoire qui produit une preuve arborescente. La question peut donc être tournée autrement comme suit : quelle est la complexité des arbres pouvant être produits par l'éliminateur de coupures ? C'est une question qui englobe la précédente, car n'importe quelle fonction numérique peut être encodée en un arbre étiqueté comme à la Figure 7.1, où les branches successives partant de la tige principale encodent les différentes valeurs de $f(n)$.

Cette approche ramène le problème à celui de comparer le fonctionnement de l'éliminateur de coupures au fonctionnement d'autres modèles d'automates finis avec mémoire qui produisent des arbres. Un choix particulièrement intéressant de telles machines est celui des automates à pile d'ordre supérieur (Knapik *et al.*, 2002). La hiérarchie de Caucal (Caucal, 2003) est une classification bien établie

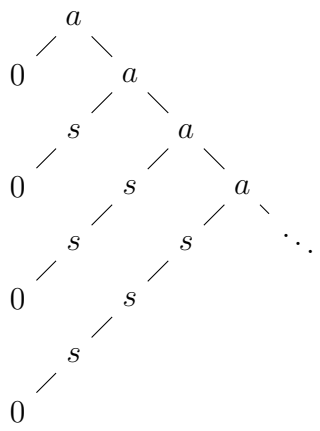


Figure 7.1 Un arbre étiqueté pour encoder la fonction identité

d'arbres infinis à branchements finis. Le niveau d'un arbre dans cette hiérarchie correspond au niveau de complexité de la structure de mémoire de l'automate d'ordre supérieur qui l'engendre. Ces structures de mémoire sont des piles de piles de ... de piles. L'idée est donc de situer les arbres produits par l'éliminateur de coupure dans la hiérarchie.

Il se trouve, comme on le démontre dans le présent chapitre, que tous les arbres se trouvant dans la hiérarchie de Caucal peuvent être calculés par l'éliminateur de coupures, qui opère sur une pré-preuve finie. On démontre ce fait par une construction explicite de la pré-preuve en question. Cela ne signifie toutefois pas que les arbres d'ordre supérieur peuvent tous être *dénotés* par des preuves circulaires, car notre construction ne satisfait pas nécessairement la condition de garde (ce qui n'empêche pas l'élimination des coupures d'être productive). On doit donc faire une distinction entre les arbres qui sont *circulairement calculables* et ceux qui sont *circulairement définissables*. On démontre aussi que la réciproque est fausse, en exhibant un arbre circulairement définissable qui ne se trouve pas dans la hiérarchie de Caucal.

Les résultats de ce chapitre sont présentés dans (Fortier, 2015).

7.1 Σ-arbres

Fixons une signature Σ, c'est-à-dire un ensemble muni d'une fonction d'arité $\mathrm{ar} : \Sigma \to \mathbb{N}$. Les Σ-arbres sont des arbres étiquetés par Σ en respectant l'arité, plutôt que simplement par un alphabet.

Définition. Un ***Σ-arbre*** est un tuple $t = (f, t_1 \dots t_r)$ tel que $f \in \Sigma$, $r = \mathrm{ar}(f)$ et $t_1 \dots t_r$ sont des Σ-arbres.

La précédente définition est, bien sûr, circulaire, mais nous ne sommes plus étrangers aux objets définis circulairement, n'est-ce pas ? Afin de permettre les Σ-infinis, on précise la définition en spécifiant qu'on considère le plus grand point fixe de celle-ci.

Cela mérite d'être formalisé par un système dirigé d'équations. Soit $\mathcal{T}$ le système constitué des équations suivantes :

$$T =_2 \coprod_{f \in \Sigma} f \qquad , \qquad f =_2 \prod_{j=1}^{\mathrm{ar}(f)} T \quad (\forall f \in \Sigma). \tag{7.1}$$

Alors pour exhiber un élément de $t \in [\![T]\!]$, on doit choisir un symbole $f \in \Sigma$, puis exhiber un élément de $[\![f]\!]$. Or, cela revient à choisir $\mathrm{ar}(f)$ éléments de $[\![T]\!]$ puis les exhiber. Ainsi, t est déterminé par un choix d'éléments $(f, t_1 \dots t_{\mathrm{ar}(f)})$, comme dans la définition d'un Σ-arbre. Le fait de prendre une priorité paire signifie qu'on permet à ce processus de se produire une infinité de fois, permettant ainsi les branches infinies.

Définition. Un Σ-arbre t est *circulairement définissable* s'il existe une preuve circulaire close Π sur un système $\mathcal{S} \supseteq \mathcal{T}$ et un sommet $u \in \Pi$ tel que $\textsc{Seq}(u) = 1 \vdash T$ et $[\![u]\!]_\Pi : \mathbf{1} \to T$ prend la valeur t. On dénote par **CD** l'ensemble des Σ-arbres circulairement définissables.

Un simple argument de cardinalité démontre que la plupart des Σ-arbres ne sont pas circulairement définissables. On peut toutefois les représenter par des preuves arborescentes, par le Théorème 6.4. On rappelle, dans la Figure 7.2, comment Ψ_t est défini, pour un Σ-arbre t.

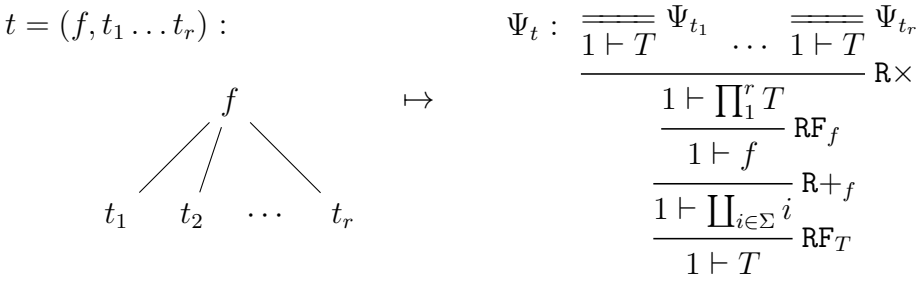


Figure 7.2 Représentation des Σ-arbres en preuves

Notons qu'afin de simplifier l'écriture, on s'est permis de généraliser la forme des règles de produits et de coproduits pour permettre de l'appliquer sur les produits ou coproduits finis quelconques, plutôt que seulement binaires (voir le Tableau 7.1). Le passage d'une forme à l'autre se fait par une récurrence évidente. Notons qu'avec cette nouvelle notation, les règles `LAx` et `RAx` sont des instances de L+ et R× respectivement, avec un coproduit (resp. produit) vide.

	$\mathfrak{L}$	$\mathfrak{R}$
Produit ($j \in I$)	$\dfrac{A_j \vdash B}{\prod_{i\in I} A_i \vdash B}\,\mathtt{L}\times_j$	$\dfrac{\{A \vdash B_i\}_{i\in I}}{A \vdash \prod_{i\in I} B_i}\,\mathtt{R}\times$
Coproduit ($j \in I$)	$\dfrac{\{A_i \vdash B\}_{i\in I}}{\coprod_{i\in I} A_i \vdash B}\,\mathtt{L}+$	$\dfrac{A \vdash B_j}{A \vdash \coprod_{i\in I} B_i}\,\mathtt{R}+_j$

Tableau 7.1 Forme générale des règles de produit et de coproduit

Définition. Un Σ-arbre t est *circulairement calculable* s'il existe une pré-preuve close et finie Π ainsi qu'une multicoupure $M \in \mathcal{M}_\Pi$ telle que $\mathrm{CE}_\Pi(M) = \Psi_t$. Soit **CC** l'ensemble des Σ-arbres circulairement calculables.

Il faut noter qu'on n'exige pas, dans la définition précédente, que Π satisfasse la condition de garde. Il n'y a donc pas de garantie, *a priori*, que $\mathrm{CE}_\Pi(M)$ soit bien défini, mais on se restreint aux situations où c'est le cas.

Proposition 7.1. $\mathbf{CD} \subseteq \mathbf{CC}$. *(La réciproque n'est pas claire...)*

Démonstration. Soit $t \in \mathbf{CD}$. Alors il existe une preuve circulaire close Π et un sommet $u \in \Pi$ tels que $[\![u]\!]_\Pi : \mathbf{1} \to [\![T]\!]$ prend la valeur t. Par le Théorème 6.10, on a donc $\mathrm{CE}_\Pi(u) = \Psi_t$, d'où $t \in \mathbf{CC}$. □

7.2 Algèbre des n-piles

Les automates d'ordre supérieur opèrent sur des piles d'ordre supérieur, qu'on appelle des n-piles. Avant de passer à la définition des automates eux mêmes, il importe d'étudier les piles ainsi que leur structure algébrique.

Définition. Fixons un alphabet fini Γ avec un symbole $\perp \in \Gamma$. Une ***0-pile*** est un élément de Γ. Pour $n \geq 1$, une ***n-pile*** est une liste finie de $(n-1)$-piles. Une n-pile est dite *bien formée* si $n = 0$ ou si elle est une liste *non vide* de $(n-1)$-piles bien formées. Le ***symbole de dessus*** d'une n-pile bien formée est défini récursivement comme suit :

$$\mathtt{top}(a) = a \quad (a \in \Gamma) \qquad ; \qquad \mathtt{top}[s_\ell, s_{\ell-1} \dots s_1] = \mathtt{top}(s_\ell).$$

Il s'agit essentiellement de la même définition que dans (Knapik *et al.*, 2002), sauf que dans cette dernière, on exige des n-piles qu'elles soient toujours bien

formées. Cela ne fera aucune différence pour nos besoins, puisque les opérations qu'on définira sur les n-piles seront des fonctions partielles. Le cas des n-piles qui ne sont pas bien formées sera traité comme une erreur.

On doit d'abord décrire les n-piles par un système d'équations dirigé, afin de les manipuler par les preuves circulaires. Puisque les n-piles sont des listes finies de $(n-1)$-piles, la première solution à laquelle on pourrait penser serait d'itérer l'étoile de Kleene, $P^* = \mu X.(1 + P \times X)$, qui définit le monoïde libre. On aurait donc la définition récursive suivante de l'ensemble P_n des n-piles :

$$P_0 := \Gamma \ ,$$
$$P_{n+1} := P_n^* =_\mu 1 + (P_n \times P_n^*) \ .$$

Or, ce système ne conviendra pas à nos besoins, puisque les produits cartésiens se traitent mal du côté gauche des preuves circulaires. En effet, la structure des règles $\mathtt{L}\times_j$ nous oblige à sacrifier la queue d'une telle liste pour pouvoir lire sa tête, et vice-versa.

On contourne ce problème en définissant plutôt le monoïde libre dans la catégorie $\mathcal{V} = \mathcal{End}(\mathcal{Ens})$ des endofoncteurs de la catégorie des ensembles, plutôt que de le faire dans la catégorie des ensembles elle-même. On se souviendra, de (Mac Lane, 1998, Chap. VII), que $\mathcal{V}$ est une catégorie monoïdale stricte dont le produit tensoriel est donné par la composition $\circ$ des foncteurs. Un monoïde dans $\mathcal{V}$ s'appelle une *monade*.

Un foncteur $F \in \mathcal{V}$ est dit ***définissable*** s'il existe un μ-terme r, avec une seule variable libre X, tel que $F = \|r\|_{\{X\}}$. Étant donné un tel foncteur, on peut montrer (voir Cockett et Santocanale, 2003) que le foncteur $\widehat{F}(X) := \mu Y.(X + F(Y))$ a la structure d'une monade libre. On définit alors la famille suivante de foncteurs :

$$S_0(X) = \coprod_{a \in \Gamma} X \qquad , \qquad S_n(X) = \widehat{S}_{n-1}(X)$$

Ainsi, pour tout $n \geq 1$, $S_n(X)$ est une algèbre initiale paramétrique dont la structure est la suivante :

$$\alpha_X^n = \{\mathtt{Nil}_X^n, \mathtt{Cons}_X^n\} \ : \ X + S_{n-1}S_n(X) \longrightarrow S_n(X).$$

Par une simple récurrence sur k, les foncteurs

$$[\![Z_k]\!] = S_k \circ S_{k+1} \circ \ldots \circ S_n \qquad (0 \leq k \leq n)$$

forment une solution au système dirigé suivant :

$$\mathcal{Z}_n(X) = \left\{ \begin{array}{ll} Z_{n+1} = & X \\ Z_k =_1 & Z_{k+1} + Z_{k-1} \qquad (0 \leq k \leq n) \\ Z_0 =_1 & \coprod_{a \in \Gamma} Z_1 \end{array} \right\}.$$

Ce système a une variable libre, X, qu'on instanciera par l'ensemble de notre choix. Par abus de notation, dans les preuves utilisant le système $\mathcal{Z}_n(X)$, on se permettra d'écrire $S_k \cdots S_n X$ au lieu de Z_k, ou simplement $S_k \cdots S_n$ si $X = 1$.

Lemme 7.2. *Pour tout $n \in \mathbb{N}$ et tout ensemble X, $S_n(X) \cong P_n \times X$. En particulier, $S_n(\mathbf{1})$ représente l'ensemble des n-piles.*

Démonstration. Par le Théorème 2.10, $S_n(X) = [\![Z_n]\!](X)$ est isomorphe à l'ensemble des stratégies gagnantes déterministes pour le joueur σ, à partir de la position Z_n, dans le jeu de parité $J_n := J(\mathcal{Z}_n(X))$ correspondant (revoir la Section 2.5).

Le jeu J_0 est illustré à la Figure 7.3, où la double flèche signifie qu'il y a une transition pour chaque symbole $a \in \Gamma$.

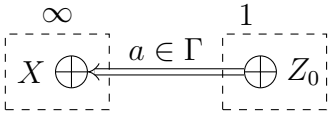


Figure 7.3 Jeu de parité associé à $\mathcal{Z}_0(X)$

Pour $n \geq 1$, le jeu J_n est représenté à la Figure 7.4. La hauteur des sommets de ce jeu est 0 sur la première rangée et ∞ sur la seconde.

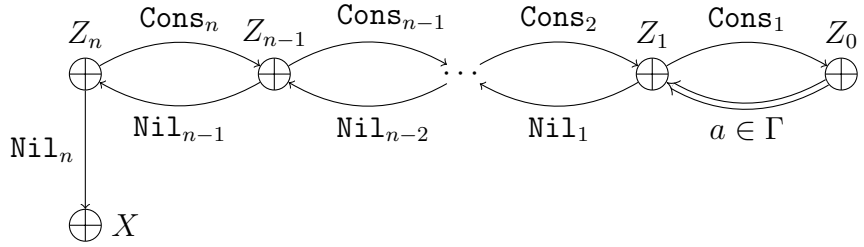


Figure 7.4 Jeu de parité associé à $\mathcal{Z}_n(X)$

Puisque c'est toujours à σ de jouer dans le jeu J_n, une stratégie gagnante est simplement une paire (s, x) où $x \in X$ et s est un chemin fini de Z_n vers $X = Z_{n+1}$. On montre par induction sur n que ces chemins sont en correspondance avec les n-piles.

Soit L_n l'ensemble des mots décrivant un chemin allant de Z_n vers Z_{n+1} (par les transitions du graphe) dans le jeu J_n. Puisque le jeu J_0 ne contient que les transitions de Z_0 vers Z_1 étiquetées par les $a \in \Gamma$, alors $L_0 = \Gamma = P_0$. Pour $n \geq 1$, clairement, les seuls mots $s \in L_n$ sont $\mathtt{Nil}_n$ et les mots de la forme $\mathtt{Cons}_n \cdot u \cdot v$ où $u \in L_{n-1}$ et $v \in L_n$. On a donc

$$L_n = (\mathtt{Cons}_n \cdot L_{n-1})^* \cdot \mathtt{Nil}_n \cong (L_{n-1})^*.$$

Par induction, on a $L_{n-1} \cong P_{n-1}$ et donc, $L_n \cong P_{n-1}^* = P_n$. □

La notation utilisée dans la preuve du Lemme 7.2 permet aussi d'obtenir le prochain lemme utile.

Définition. Une preuve circulaire Λ est ***linéaire*** si elle est arborescente et si chaque sommet de Λ est de degré 1.

Lemme 7.3. *Pour toute n-pile $s \in S_n(\mathbf{1})$, il existe une unique preuve linéaire finie Λ_s sur $\mathcal{Z}_n(1)$, telle que* $\textsc{Seq}(r_n) = 1 \vdash S_n(1)$ *et* $[\![\Lambda_s]\!] : \mathbf{1} \vdash S_n(\mathbf{1})$ *prend la valeur s. La racine de Λ_s sera dénotée $\sqrt{s}$.*

Démonstration. Soit $s \in S_n(\mathbf{1})$. Par le Théorème 6.4, il existe une preuve arborescente Λ_s telle que $[\![\Lambda_s]\!] = s$. Or, par le Lemme 5.4, les seules règles qu'on peut utiliser dans Λ_s sont des règles droite. Or, par inspection du système $\mathcal{Z}_n(1)$, les seules règles admissibles sont les $\mathtt{RF}_{Z_k}$ et les $\mathtt{R}{+}_j$ (toutes de degré 1). Enfin, par le Lemme 6.1, Λ_s est une preuve finie. Enfin, l'unicité découle de la Proposition 6.5.

Il est quand même utile d'exhiber la construction de Λ_s qui est proposée dans le Théorème 6.4. Rappelons que, selon la représentation du Lemme 7.2, s est identifié à un mot de L_n. Chaque lettre de s correspond à un mouvement dans le jeu correspondant. On peut encoder ces mouvements dans une preuve comme suit :

– si $s = \mathtt{Nil}_n$, alors

$$\Lambda_s = \dfrac{\dfrac{\dfrac{}{1 \vdash 1}\,\mathtt{RAx}}{1 \vdash 1 + Z_{n-1}}\,\mathtt{R}{+}_0}{1 \vdash Z_n}\,\mathtt{RF}_{Z_n} \;;$$

– si $s = \mathtt{Cons}_k \cdot w$, alors

$$\Lambda_s = \dfrac{\dfrac{\dfrac{}{1 \vdash Z_{k-1}}\,\Lambda_w}{1 \vdash Z_{k+1} + Z_{k-1}}\,\mathtt{R}{+}_1}{1 \vdash Z_k}\,\mathtt{RF}_{Z_k} \;;$$

– si $s = \mathtt{Nil}_k \cdot w$ avec $k < n$, alors

$$\Lambda_s = \dfrac{\dfrac{\dfrac{}{1 \vdash Z_{k+1}}\,\Lambda_w}{1 \vdash Z_{k+1} + Z_{k-1}}\,\mathtt{R}{+}_0}{1 \vdash Z_k}\,\mathtt{RF}_{Z_k} \;;$$

– si $s = a \cdot w$ avec $a \in \Gamma$, alors

$$\Lambda_s = \dfrac{\dfrac{\dfrac{}{1 \vdash Z_1}\,\Lambda_w}{1 \vdash \coprod_\Gamma Z_1}\,\mathtt{R}{+}_a}{1 \vdash Z_0}\,\mathtt{RF}_{Z_0}\ .$$

□

Notre prochain objectif est d'exprimer les opérations usuelles de n-piles dans ce modèle. L'objectif est de dégager le fait que ces opérations ne font intervenir rien d'autre que les opérations des catégories μ-bicomplètes et donc, qu'elles sont définissables par des preuves circulaires, en vertu du Théorème 4.7.

On commence par définir le *fond de n-pile* :

$$\bot_0 = \bot \in \Gamma \qquad ; \qquad \bot_{n+1} = [\bot_n].$$

Ce sont des n-piles particulières qu'on peut assimiler à des fonctions du type $\bot_n : \mathbf{1} \to S_n(\mathbf{1})$. Il suffit de prendre $\bot_n = b^n_1$, où $b^n_X : X \to S_n X$ est défini comme suit :

$$b^0_X = \mathtt{in}^X_\bot \qquad ; \qquad b^{n+1}_X = \mathtt{Nil}^n_X \cdot b^{n-1}_{S_n X} \cdot \mathtt{Cons}^n_X.$$

Une première opération consiste à *pousser* un symbole $a \in \Gamma$ au sommet d'une 1-pile. En pratique, on n'utilisera cette opération qu'avec un symbole $a \neq \bot$ afin que $\bot$ n'agisse strictement qu'en tant que symbole de fond de pile.

$$\mathtt{spush}^a_1[a_\ell, a_{\ell-1} \ldots a_1] = [a, a_\ell, a_{\ell-1} \ldots a_1].$$

Il s'agit simplement de $p^a_{1;1}$, où $p^a_{1;X}$ est défini par le composition suivante :

$$S_1 X \xrightarrow{\mathtt{in}^{S_1 X}_a} \coprod_{a \in \Gamma} S_1 X = S_0 S_1 X \xrightarrow{\mathtt{Cons}^1_X} S_1 X \hookrightarrow X + S_1 X.$$

Pour les autres opérations, on a besoin d'une propriété supplémentaire des foncteurs S_n qu'on peut dériver de (Cockett et Santocanale, 2003) : ce sont des *comonades cocommutatives*.

Définition. Un foncteur $F \in \mathcal{V}$ est ***central*** s'il existe une collection de transformations naturelles $\phi^F = (\phi^F_G)_{G \in \mathcal{V}}$ telle que pour chaque $\phi^F_G : F \circ G \to G \circ F$, on a $\phi^F_I = \mathtt{id}_F$ et $\phi^F_{GH} = (\phi^F_G H) \cdot (G \phi^F_H)$.

Dans (Cockett et Santocanale, 2003), il est démontré que les foncteurs S_n sont tous centraux (précisément, c'est une conséquence de l'Exemple 4.2 et de la Proposition 4.3). On ne fait que rappeler ici la définition des transformations naturelles $\phi^{S_n}_G = (\phi^{S_n}_{G;X})_{X \in \mathcal{Ens}}$ afin de vérifier qu'on peut les définir par des preuves circulaires.

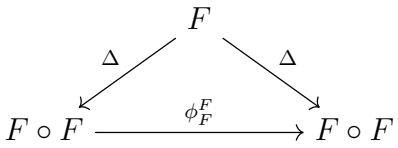
Si $n = 0$, on définit $\phi^{S_0}_{G;X} = \{G(\mathtt{in}^X_a)\}_{a \in \Gamma}$. Pour $n \geq 1$, $\phi^{S_n}_{G;X}$ est défini par récurrence sur n en tant que l'unique fonction faisant commuter le diagramme suivant (elle existe par initialité de α^n_{GX}).

$$\begin{array}{ccc}
G(X) + S_{n-1}S_nG(X) & \xrightarrow{\mathtt{id}_{GX} + S_{n-1}\phi^{S_n}_{G;X}} & G(X) + S_{n-1}GS_n(X) \\
 & & \downarrow{\scriptstyle \mathtt{id}_{GX} + \phi^{S_{n-1}}_{G;S_nX}} \\
\downarrow{\scriptstyle \alpha^n_{GX}} & & G(X) + GS_{n-1}S_n(X) \\
 & & \downarrow{\scriptstyle G\alpha^n_X} \\
S_nG(X) & \xrightarrow{\phi^{S_n}_{G;X}} & GS_n(X)
\end{array}$$

Définition. Soit $I \in \mathcal{V}$ le foncteur identité. Une ***comonade*** est un endofoncteur $F \in \mathcal{V}$ muni de deux transformations naturelles $\Upsilon : F \to I$ et $\Delta : F \to F \circ F$, appelées respectivement ***destructeur*** et ***doubleur***, telles que les diagrammes suivants commutent.

$$\begin{array}{ccc}
 & F & \\
{\scriptstyle \Delta}\swarrow & & \searrow{\scriptstyle \Delta} \\
F \circ F & & F \circ F \\
\downarrow{\scriptstyle \mathtt{id}_F \circ \Delta} & & {\scriptstyle \Delta \circ \mathtt{id}_F}\downarrow \\
F \circ (F \circ F) & = & (F \circ F) \circ F
\end{array}
\qquad\qquad
\begin{array}{ccccc}
I \circ F & \xleftarrow{\Upsilon \circ \mathtt{id}_F} & F \circ F & \xrightarrow{\mathtt{id}_F \circ \Upsilon} & F \circ I \\
 & \searrow & \uparrow{\scriptstyle \Delta} & \swarrow & \\
 & & F & &
\end{array}
\tag{7.2}$$

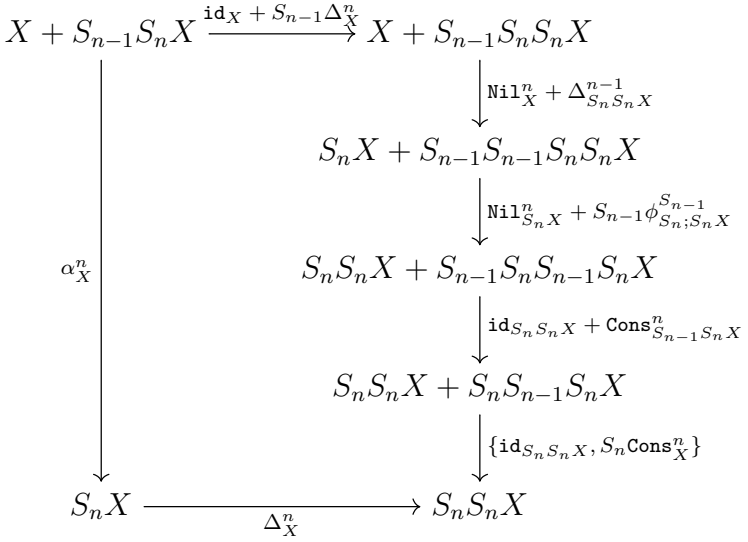
Une comonade F est *cocommutative* si F est central et le diagramme suivant commute.



Par exemple, le foncteur S_0 est une comonade cocommutative, où les transformations naturelles $\Upsilon^0 = \{\Upsilon^0_X\}_{X \in \mathcal{E}ns}$ et $\Delta^0 = \{\Delta^0_X\}_{X \in \mathcal{E}ns}$ sont données par les équations suivantes :

$$\Upsilon^0_X = \{\mathtt{id}_X\}_{a \in \Gamma} \qquad ; \qquad \Delta^0_X = \{\mathtt{in}_a^{S_0(X)} \mathtt{in}_a^X\}_{a \in \Gamma}.$$

Il découle, par (Cockett et Santocanale, 2003, Prop. 4.6), que chaque foncteur S_n est une comonade cocommutative. Encore une fois, on ne fait que rappeler la définition Υ^n et Δ^n dans cet article. Il s'agit, encore une fois, d'une définition récursive sur n. Pour tout ensemble X, Δ^n_X est l'unique fonction telle que le diagramme suivant commute.



Quant à Υ^n_X, il s'agit de l'unique fonction telle que le diagramme suivant commute.

$$\begin{array}{ccc} X + S_{n-1}S_nX & \xrightarrow{\mathtt{id}_X + S_{n-1}\Upsilon^n_X} & X + S_{n-1}X \\ \Big\downarrow{\scriptstyle \alpha^n_X} & & \Big\downarrow{\scriptstyle \{\mathtt{id}_X, \Upsilon^{n-1}_X\}} \\ S_nX & \xrightarrow[\Upsilon^n_X]{} & X \end{array}$$

Lemme 7.4. *Pour tout ensemble X, il existe des fonctions* définissables par des preuves circulaires $\Upsilon^n_X : S_nX \to X$ *et* $\Delta^n_X : S_nX \to S_nS_nX$ *telles que pour tout* $(s, x) \in S_nX$, $\Upsilon^n_X(s, x) = x$ *et* $\Delta^n_X(s, x) = (s, (s, x))$.

Démonstration. Il devrait être clair, au vu des définitions diagrammatiques ci-dessus, que Υ^n_X et Δ^n_X sont définissables par des preuves circulaires, puisque leur définition n'utilise rien d'autre que la structure μ-bicomplète de la catégorie des ensembles. Quant aux équations recherchées, on les obtient grâce aux diagrammes de comonade (7.2). En effet, soit $(s_0, (s_1, y)) = \Delta^n_X(s, x)$. Soit ensuite s'_0, s'_1, y' tels que

$$(\Delta^n_X \circ \mathtt{id}_{S_n}) = (s'_0, (s'_1, (s_1, y))),$$
$$(\mathtt{id}_{S_n} \circ \Delta^n_X) = (s_0, (s'_0, (s'_1, y'))).$$

Par (7.2), on a $s_0 = s'_0 = s'_1 = s_1$ et $y = y'$. Donc soit donc $s' = s_0$. On a alors $\Delta^n_X(s, x) = (s', (s', y))$. Par l'autre diagramme de (7.2), on a

$$(\mathtt{id}_{S_n} \circ \Upsilon^n_X)(s', (s', y)) = (s, x)$$

et donc $s' = s$ et $\Upsilon^n_X(s', y) = x$. Enfin, on a

$$(\Upsilon^n_X \circ \mathtt{id}_{S_n})(s, (s, y)) = (s, x)$$

et donc $y = x$. □

Revenons à la question de définir les opérations usuelles sur les n-piles. Pour une pile de n'importe quel niveau, on peut opérer les opérations `push` et `pop` définies comme suit :

$$\begin{aligned}\mathtt{push}_n^n[s_\ell, s_{\ell-1} \dots s_1] &= [s_\ell, s_\ell, s_{\ell-1} \dots s_1];\\ \mathtt{pop}_n^n[s_\ell, s_{\ell-1} \dots s_1] &= [s_{\ell-1} \dots s_1].\end{aligned}$$

Chacune de ces deux opérations est de la forme $p^n_{n;1}$, où la famille de fonctions $p^n_{n;X} : S_nX \to X + S_nX$ est de la forme $p^n_{n;X} = (\alpha^n_X)^{-1}\cdot(\mathtt{id}+f)$. La différence entre $\mathtt{push}^n_n$ et $\mathtt{pop}^n_n$ est donc le choix de la fonction $f : S_{n-1}S_nX \to S_nX$ dans cette dernière expression. Pour $\mathtt{pop}^n_n$, puisqu'on veut *détruire* une certaine information, on prend $f = \Upsilon^{n-1}_{S_nX}$. Pour $\mathtt{push}^n_n$, puisqu'on veut *doubler* la première $(n-1)$-pile, on choisit comme f la composition suivante :

$$S_{n-1}S_nX \xrightarrow{\Delta^{n-1}_{S_nX}} S_{n-1}S_{n-1}S_nX \xrightarrow{S_{n-1}(\mathtt{Cons}^n_X)} S_{n-1}S_nX \xrightarrow{\mathtt{Cons}^n_X} S_nX.$$

Enfin, on a besoin des opérations suivantes de niveau $k < n$:

$$\begin{aligned}\mathtt{spush}^a_n[s_\ell, s_{\ell-1} \dots s_1] &= [\mathtt{spush}^a_{n-1}(s_\ell), s_{\ell-1} \dots s_1];\\ \mathtt{push}^k_n[s_\ell, s_{\ell-1} \dots s_1] &= [\mathtt{push}^k_{n-1}(s_\ell), s_{\ell-1} \dots s_1];\\ \mathtt{pop}^k_n[s_\ell, s_{\ell-1} \dots s_1] &= [\mathtt{pop}^k_{n-1}(s_\ell), s_{\ell-1} \dots s_1].\end{aligned}$$

La forme de ces trois définitions est la même. Ce sont des fonctions de la forme $p^z_{n;1}$, où $p^z_{n;X} : S_nX \to X + S_nX$ est soit déjà défini plus haut, ou peut être atteint par induction sur n, en définissant $p^z_{n;X} = (\alpha^n_X)^{-1} \cdot (\mathtt{id} + f)$, où f est la composition suivante

$$S_{n-1}S_nX \xrightarrow{p^z_{n-1;S_nX}} S_nX + S_{n-1}S_nX \xrightarrow{v_n+\mathtt{id}} X + S_{n-1}S_nX \xrightarrow{\alpha^n_X} S_nX,$$

dans laquelle $v_n : S_nX \to X$ est la fonction $(s, x) \mapsto x$.

L'ensemble des ***opérations de niveau*** n est alors défini comme suit :

$$\mathcal{O}_n = \{\mathtt{spush}^a_n : a \in \Gamma \setminus \{\bot\}\} \cup \{\mathtt{push}^k_n, \mathtt{pop}^k_n : 1 \le k \le n\}.$$

7.3 Simulation d'automates d'ordre supérieur

Définition. Un ***automate à pile de niveau*** n (abbrévié n-AP) est un tuple $\mathcal{A} = \langle Q, \Sigma, \Gamma, q_0, \delta \rangle$, où Q est un ensemble fini d'états, avec un état initial $q_0 \in Q$, Γ est un alphabet fini pour la pile, Σ est une signature et $\delta : Q \times \Gamma \to \mathcal{I}_\mathcal{A}$ est la ***fonction de transition***.

Dans la dernière définition, $\mathcal{I}_\mathcal{A}$ est l'ensemble des *instructions admissibles*, constitué des expressions de l'une des deux formes suivantes :
– (q, θ), où $q \in Q$ et $\theta \in \mathcal{O}_n$;
– $(f, p_1 \dots p_r)$, où $f \in \Sigma$, $r = \mathrm{ar}(f)$ et $p_1 \dots p_r \in Q$.
Une *configuration* de $\mathcal{A}$ est une paire (q, s) où $q \in Q$ et s est une n-pile. Soit $\mathcal{C}_\mathcal{A}$ l'ensemble de toutes les configurations de $\mathcal{A}$. On écrit $(q, s) \to_\mathcal{A} (q', s')$ si $\delta(q, \mathtt{top}(s)) = (q', \theta)$ pour un certain $\theta \in \mathcal{O}_n$ tel que $s' = \theta(s)$. La relation $\twoheadrightarrow_\mathcal{A}$ est la fermeture réflexive transitive de $\to_\mathcal{A}$.

Soit $t = (f, t_1 \dots t_r)$ un Σ-arbre et $(q, s) \in \mathcal{C}_\mathcal{A}$. Une *exécution de t à partir de (q, s)* est une fonction partielle $\varrho : T \rightharpoonup \mathcal{C}_\mathcal{A}$ définie en t, avec la propriété suivante. Soit $\varrho(t) = (q_t, s_t)$. Alors $(q, s) \twoheadrightarrow_\mathcal{A} (q_t, s_t)$ et $\delta(q_t, \mathtt{top}(s_t)) = (f, p_1 \dots p_r)$ pour certains états $p_1 \dots p_r \in Q$ tels que pour $1 \leq i \leq r$, ϱ est une exécution de t_i à partir de (p_i, s_t). Un Σ-arbre t est *accepté* par $\mathcal{A}$ si et seulement s'il y a une exécution de t à partir de $(q_0, \bot_n)$. Puisque nos automates sont déterministes, on peut conclure qu'un n-AP accepte au plus un seul Σ-arbre.

On montre maintenant comment convertir un n-AP $\mathcal{A} = \langle Q, \Sigma, \Gamma, q_0, \delta \rangle$ en une pré-preuve finie $\Pi(\mathcal{A})$. L'idée générale est de reproduire la structure de graphe de $\mathcal{A}$ dans celle de $\Pi(\mathcal{A})$, tout en remplaçant chaque sommet par un *gadget* qui simule son comportement. Pour cela, on maintient la n-pile du côté gauche du symbole $\vdash$ tandis que l'arbre sera maintenu à droite.

Afin de traiter les cas d'erreurs possibles, on voit plutôt t comme un Σ'-arbre, où $\Sigma' = 1 + \Sigma$. Cela nous permet de définir une preuve $\mathtt{err}_X$ pour n'importe quelle formule X de la façon suivante :

$$\mathtt{err}_X = \dfrac{\dfrac{\dfrac{}{X \vdash 1}\,\mathtt{RAx}}{X \vdash 1 + \coprod_{f\in\Sigma} f}\,\mathtt{R}{+_0}}{X \vdash T}\,\mathtt{RF}_T\,.$$

On encode premièrement la fonction de transition δ par une preuve $\widetilde{\delta}$. L'encodage dépend de la forme de $\delta(q,a)$ comme suit :

– si $\delta(q,a) = (\theta, p)$ pour $\theta \in \mathcal{O}_n$, alors

$$\widetilde{\delta}(q,a) = \dfrac{\dfrac{}{S_n 1 \vdash 1 + S_n 1}\,\theta \qquad \dfrac{\dfrac{}{1 \vdash T}\,\mathtt{err}_1 \qquad \dfrac{}{S_n 1 \vdash T}\,\mathtt{H}}{1 + S_n 1 \vdash T}\,\mathtt{L}+}{S_n 1 \vdash T}\,\mathtt{C}\,;$$

– si $\delta(q,a) = (f, p_1 \dots p_r)$ pour $f \in \Sigma$, alors

$$\widetilde{\delta}(q,a) = \dfrac{\dfrac{\dfrac{}{S_n 1 \vdash T}\,\mathtt{H}_1 \quad \cdots \quad \dfrac{}{S_n 1 \vdash T}\,\mathtt{H}_r}{S_n 1 \vdash \prod_1^r T}\,\mathtt{R}\times}{S_n 1 \vdash f}\,\mathtt{RF}_f}{S_n 1 \vdash 1 + \coprod_{i\in\Sigma} i}\,\mathtt{R}{+_f}}{S_n 1 \vdash T}\,\mathtt{RF}_T\,.$$

Dans $\mathcal{A}$, le choix de la transition à emprunter dépend du symbole de dessus de n-pile. Ainsi, on veut une preuve $\mathtt{TOP}$ avec autant d'hypothèses que la cardinalité de Γ, qu'on peut utiliser pour brancher sur les différents cas.

Pour ce faire, on doit d'abord « creuser » dans la n-pile afin d'aller y dénicher le

symbole du dessus. On définit donc $\mathtt{DIG}_k$ comme suit :

$$\mathtt{DIG}_0 = \dfrac{\left\{ \dfrac{}{X \vdash T}\,\mathtt{H}_a \right\}_{a\in\Gamma}}{\dfrac{\coprod_\Gamma X \vdash T}{S_0X \vdash T}\,\mathtt{LF}_{S_0X}}\,\mathtt{L}+\,,$$

$$\mathtt{DIG}_k = \dfrac{\dfrac{}{X \vdash T}\,\mathtt{err}_X \qquad \dfrac{\left\{ \dfrac{}{(S_1\cdots S_k)X \vdash T}\,\mathtt{H}_a \right\}_{a\in\Gamma}}{S_{k-1}S_kX \vdash T}\,\mathtt{DIG}_{k-1}[X/S_kX]}{\dfrac{X + S_{k-1}S_kX \vdash T}{S_kX \vdash T}\,\mathtt{LF}_{S_kX}}\,\mathtt{L}+\,.$$

Lemme 7.5. *Soit $s \in S_n(\mathbf{1})$ une n-pile bien formée et soit $\mathtt{top}(s) = a$. Soit $\Pi = \mathtt{DIG}_n[X/1]$ dont la racine est dénotée u et les hypothèses sont $(v_i)_{i\in\Gamma}$. Alors, dans $\mathcal{M}_{\Lambda_s\cup\Pi}$, on a $[\sqrt{s}, u] \overset{*}{\nsim} [\sqrt{w}, v_a]$, où $w = \mathtt{pop}_1^n(s)$.*

Démonstration. Selon la correspondence entre les n-piles et les mots du Lemme 7.2, on a

$$s = \mathtt{Cons}_n\mathtt{Cons}_{n-1}\cdots\mathtt{Cons}_1 \cdot a \cdot w.$$

On a donc $s = s_n$, où s_k est défini récursivement comme suit :

$$s_0 = a \cdot w \qquad , \qquad s_k = \mathtt{Cons}_k \cdot s_{k-1} \qquad (k \geq 1)$$

Observons que, sur $\mathcal{Z}_n(1)$, on a $\mathtt{DIG}_n[X/1] = \Pi_n$, où Π_k est défini comme suit.

$$\Pi_0 = \dfrac{\left\{ \dfrac{}{v_i : Z_1 \vdash T}\,\mathtt{H}_i \right\}_{i\in\Gamma}}{\dfrac{\coprod_\Gamma Z_1 \vdash T}{u_0 : Z_0 \vdash T}\,\mathtt{LF}_{Z_0}}\,\mathtt{L}+\,,$$

$$\Pi_k = \dfrac{\dfrac{}{Z_{k+1} \vdash T}\,\mathtt{err}_{Z_{k+1}} \qquad \dfrac{\left\{ \dfrac{}{v_i : Z_1 \vdash T}\,\mathtt{H}_i \right\}_{i\in\Gamma}}{u_{k-1} : Z_{k-1} \vdash T}\,\Pi_{k-1}}{\dfrac{Z_{k+1} + Z_{k-1} \vdash T}{u_k : Z_k \vdash T}\,\mathtt{LF}_{Z_k}}\,\mathtt{L}+\,.$$

Une simple comparaison des formules à droite de Λ_{s_k} avec celles à gauche de Π_k mène alors aux relations suivantes (dans chaque cas, l'éliminateur de coupures effectue deux réductions essentielles) :

$$[\sqrt{s_0}, u_0] \overset{*}{\nleftarrow} [\sqrt{w}, v_a] \qquad , \qquad [\sqrt{s_k}, u_k] \overset{*}{\nleftarrow} [\sqrt{s_{k-1}}, u_{k-1}] \qquad (k \geq 1).$$

Puisque $[\sqrt{s}, u] = [\sqrt{s_n}, u_n]$, le résultat en découle par récurrence. □

Ensuite, puisque la lecture est destructive dans les preuves circulaires, on a besoin d'une preuve pour « remplir » le trou laissé dans l'entrée en y remettant le symbole lu, puis en construisant une nouvelle n-pile bien formée. On définit donc $\mathtt{FILL}^a_k$ comme suit :

$$\mathtt{FILL}^a_0 = \dfrac{\dfrac{\dfrac{}{X \vdash X}\,\mathtt{I}}{X \vdash \coprod_\Gamma X}\,\mathtt{R}{+}_a}{X \vdash S_0 X}\,\mathtt{RF}_{S_0 X} \quad ,$$

$$\mathtt{FILL}^a_k = \dfrac{\dfrac{\dfrac{\mathtt{FILL}^a_{k-1}[X/S_k X]}{(S_1 \cdots S_k)X \vdash S_{k-1}S_k X}}{(S_1 \cdots S_k)X \vdash X + S_{k-1}S_k X}\,\mathtt{R}{+}_1}{(S_1 \cdots S_k)X \vdash S_k X}\,\mathtt{RF}_{S_k X} \quad .$$

Lemme 7.6. *Soit w un mot qui représente un chemin de Z_1 vers X dans la Figure 7.4. Soit u la racine de $\Pi = \mathtt{FILL}^a_n[X/1]$, où $a \in \Gamma$. Alors* $\mathrm{CE}([\sqrt{w}, u]) = \Lambda_s$, *où s est la n-pile qui correspond au mot suivant :*

$$s = \mathtt{Cons}_n \mathtt{Cons}_{n-1} \cdots \mathtt{Cons}_1 \cdot a \cdot w \,.$$

Démonstration. Par construction, on a $\mathtt{FILL}^a_n = \Pi_n$, où Π_k est défini comme suit :

$$\Pi_0 = \dfrac{\dfrac{\dfrac{}{Z_1 \vdash Z_1}\,\mathtt{I}}{Z_1 \vdash \coprod_\Gamma Z_1}\,\mathtt{R}{+}_a}{Z_1 \vdash Z_0}\,\mathtt{RF}_{Z_0} \qquad , \qquad \Pi_k = \dfrac{\dfrac{\dfrac{\Pi_{k-1}}{Z_1 \vdash Z_{k-1}}}{Z_1 \vdash Z_{k+1} + Z_{k-1}}\,\mathtt{R}{+}_1}{Z_1 \vdash Z_k}\,\mathtt{RF}_{Z_k} \quad .$$

Supposons que l'éliminateur de coupures est initialisé avec $[\sqrt{w}, u]$ en mémoire. À l'exception de la règle $\mathtt{I}$ sur la feuille, toutes les règles de chaque Π_k sont des règles droites. De plus, ces règles sont les mêmes que celles qui sont utilisées dans la construction de Λ_s. Alors les $2(n+1)$ premières actions de l'éliminateur de coupures sont des productions droites, qui produisent une copie de Λ_r (excepté à la feuille), où $r = \mathtt{Cons}_n\mathtt{Cons}_{n-1}\cdots\mathtt{Cons}_1 \cdot a$.

Après ces étapes, la mémoire de l'éliminateur de coupures est de la forme $[\sqrt{w}, v]$ où $\text{RÈG}(v) = \mathtt{I}$. Donc $M \bowtie [u]$ et par le Théorème 6.10, on trouve

$$\text{CE}([\sqrt{w}, u]) = \text{CE}([\sqrt{w}]) = \Lambda_w. \qquad \square$$

On peut maintenant définir $\mathtt{TOP}$ comme suit :

$$\mathtt{TOP} = \dfrac{\left\{ \dfrac{\dfrac{}{(S_1\cdots S_n)1 \vdash S_n 1}\,\mathtt{FILL}^a_n[X/1] \quad \dfrac{}{S_n 1 \vdash T}\,\mathtt{H}_a}{(S_1\cdots S_n)1 \vdash T}\,\mathtt{C} \right\}_{a\in\Gamma}}{S_n 1 \vdash T}\,\mathtt{DIG}_n[X/1]\,.$$

Pour tout $q \in Q$, soit Π_q la preuve suivante :

$$\Pi_q = \dfrac{\left\{ \dfrac{\dfrac{}{S_n 1 \vdash T}\,\mathtt{H}_{a,1} \quad \ldots \quad \dfrac{}{S_n 1 \vdash T}\,\mathtt{H}_{a,r}}{S_n 1 \vdash T}\,\widetilde{\delta}(q,a) \right\}_{a\in\Gamma}}{S_n 1 \vdash T}\,\mathtt{TOP}\,.$$

On dénote par $\sqrt{q}$ la racine de Π_q et par $\mathscr{D}^{a,i}_q$ l'hypothèse étiquetée par $\mathtt{H}_{a,i}$. Soit aussi $\Pi_\perp$ la preuve suivante, dont la racine est dénotée $\sqrt{\perp}$ et l'hypothèse $\mathscr{D}_\perp$:

$$\Pi_\perp = \dfrac{\dfrac{}{1 \vdash S_n 1}\,\perp_n \qquad \dfrac{}{S_n 1 \vdash T}\,\mathtt{H}}{1 \vdash T}\,\mathtt{C}\,.$$

La pré-preuve $\Pi(\mathcal{A})$ est obtenue en prenant l'union de $\Pi_\perp$ avec tous les Π_q, puis en reliant $\mathscr{D}_\perp$ à $\sqrt{q_0}$ et, pour tout $q \in Q$ et $a \in \Gamma$:

– si $\delta(q,a) = (p,\theta)$, relier $\mathscr{P}_q^{a,1}$ à $\sqrt{p}$;
– sinon, relier $\mathscr{P}_q^{a,i}$ à $\sqrt{p_i}$.

On peut maintenant énoncer le résultat principal de ce chapitre : les arbres acceptés par des n-APs sont circulairement calculables.

Théorème 7.7. *Soit $\mathcal{A}$ un n-AP qui accepte un Σ-arbre t. Alors*

$$\mathrm{CE}_{\Pi(\mathcal{A})}(\sqrt{\bot}) = \Psi_t.$$

L'idée de la preuve du Théorème 7.7 est de relever le comportement local d'une exécution $\varrho : [\![T]\!] \rightharpoonup \mathcal{C}_{\mathcal{A}}$ vers l'ensemble des configurations de l'éliminateur de coupures, c'est-à-dire, $\mathcal{M}_{\Pi(\mathcal{A})}$.

Définition. Une multicoupure $M = [u_1, u_2 \dots u_m]$ sur $\Pi(\mathcal{A})$ est ***bonne*** si elle est telle que $\textsc{Seq}_{\mathtt{L}}(u_1) = 1$ et $u_m = \sqrt{q}$ pour un certain $q \in Q$. Soit $\mathcal{M}_{\mathcal{A}}^{\heartsuit}$ l'ensemble des bonnes multicoupures sur $\Pi(\mathcal{A})$.

Selon cette définition, on peut associer à chaque bonne multicoupure M un sommet $q_M \in Q$ tel que $\sqrt{q_M}$ est le dernier élément de M.

Lemme 7.8. *Soit $M = [u_1, u_2 \dots u_m] \in \mathcal{M}_{\mathcal{A}}^{\heartsuit}$. Alors pour tout $i < m$, le graphe atteignable $\overline{(\Pi(\mathcal{A}), u_i)}$ est une preuve circulaire (qui respecte la condition de garde).*

Démonstration. Observons d'abord que par inspection, T et ses sous-formules ne peuvent apparaître qu'à la droite d'un séquent de $\Pi(\mathcal{A})$. Donc, pour tout $i < m$, $\textsc{Seq}_{\mathtt{R}}(u_i)$ n'a pas de lien avec T, car s'il en avait un, alors $\textsc{Seq}_{\mathtt{L}}(u_{i+1}) = \textsc{Seq}_{\mathtt{R}}(u_i)$ en aurait un et ce serait une contradiction.

Par construction, il s'ensuit que u_i appartient soit à une copie de $\mathtt{FILL}_n^a[X/1]$ pour un certain $a \in \Gamma$, ou à une sous-preuve qui dénote $\bot_n$ ou un certain $\theta \in \mathcal{O}_n$. Or, toutes ces preuves sont valides et donc, $\overline{(\Pi(\mathcal{A}), u_i)}$ est valide. □

Il découle du dernier résultat que pour tout $M = [u_1, u_2 \dots u_m] \in \mathcal{M}_{\mathcal{A}}^{\heartsuit}$ et $i < m$, u_i dénote une unique fonction $[\![u_i]\!]$. Puisque $\textsc{Seq}_{\mathtt{L}}(u_0) = 1$ et $\textsc{Seq}_{\mathtt{R}}(u_{m-1}) = \textsc{Seq}_{\mathtt{L}}(u_m) = S_n 1$, on peut définir $s_M : \mathbf{1} \to S_n(\mathbf{1})$ par l'équation suivante :

$$s_M = [\![u_0]\!] \cdot [\![u_1]\!] \cdots [\![u_{m-1}]\!] .$$

Si on identifie ces fonctions $\mathbf{1} \to S_n(\mathbf{1})$ aux n-piles qu'elles atteignent, on obtient une fonction $\psi : \mathcal{M}_{\mathcal{A}}^{\heartsuit} \to \mathcal{C}_{\mathcal{A}}$ définie par :

$$\psi(M) = (q_M, s_M).$$

Lemme 7.9. *Soit $M \in \mathcal{M}_{\mathcal{A}}^{\heartsuit}$ et $(q, s) = \psi(M)$. Alors pour tout $(q', s') \in \mathcal{C}_{\mathcal{A}}$ tel que $(q, s) \to_{\mathcal{A}} (q', s')$, il existe $M' \in \mathcal{M}_{\mathcal{A}}^{\heartsuit}$ tel que $M \overset{*}{\nrightarrow} M'$ et $\psi(M') = (q', s')$.*

Démonstration. Par le Lemme 6.9, on peut supposer sans perte de généralité que $M = [r_s, \sqrt{q}]$, où r_s est la racine de Λ_s. Soit $a = \mathtt{top}(s)$ et $\theta \in \mathcal{O}_n$ tel que $\delta(q, a) = (q', \theta)$ et $\theta(s) = s' \cdot \mathtt{in}_1 : \mathbf{1} \to S_n(\mathbf{1})$.

Puisque $\mathtt{top}(s)$ est supposé défini, alors s est bien formé et, en particulier, on peut représenter s dans L_n par un mot de la forme suivante :

$$s = \mathtt{Cons}_n \mathtt{Cons}_{n-1} \cdots \mathtt{Cons}_1 \cdot a \cdot w \, .$$

Identifions clairement certains sommets dans Π_q :

$$\dfrac{\left\{ \dfrac{\dfrac{}{f_b : (S_1 \cdots S_n) \vdash S_n}\,\mathtt{FILL}_n^b[X/1] \quad \dfrac{\dots \mathscr{D}_q^{b,i} : S_n \vdash T \dots}{v_b : S_n \vdash T}\,\widetilde{\delta}(q,b)}{d_b : (S_1 \cdots S_n) \vdash T}\,\mathtt{C} \right\}_{b \in \Gamma}}{\sqrt{q} : S_n \vdash T}\,\mathtt{DIG}_n[X/1] \, .$$

Souvenons-nous que $\mathscr{D}_q^{a,1} = \sqrt{q'}$ dans $\Pi(\mathcal{A})$. La preuve $\widetilde{\delta}(q, a)$ est la suivante :

$$\dfrac{\dfrac{}{y : S_n \vdash 1 + S_n}\,\theta \quad \dfrac{\dfrac{}{1 \vdash T}\,\mathtt{err}_1 \qquad \sqrt{p} : S_n \vdash T}{z : 1 + S_n \vdash T}\,\mathtt{L}+}{v_a : S_n \vdash T}\,\mathtt{C} \, .$$

En utilisant le Lemme 7.5 suivi de deux fois l'opération FUSION, on obtient :

$$[\sqrt{s}, \sqrt{q}] \overset{*}{\nleftarrow} [\sqrt{w}, d_a] \nleftarrow [\sqrt{w}, f_a, v_a] \nleftarrow [\sqrt{w}, f_a, y, z].$$

Maintenant, par le Lemme 7.6, on a $\text{CE}([\sqrt{w}, f_a]) = \Lambda_s$ et donc $[\![\sqrt{w}]\!] \cdot [\![f_a]\!] = s$. Puisque s est bien formé et puisque

$$[\![y]\!] = \theta : S_n(\mathbf{1}) \to \mathbf{1} + S_n(\mathbf{1}),$$

alors $[\![\sqrt{w}]\!] \cdot [\![f_a]\!] \cdot [\![y]\!] = \theta(s) = s' \cdot \mathtt{in}_1$. Or, voici une autre preuve qui dénote la même fonction $s' \cdot \mathtt{in}_1$:

$$\dfrac{\dfrac{\overline{\qquad\qquad} \Lambda_{s'}}{r_{s'} : 1 \vdash S_n(\mathbf{1})}}{u : 1 \vdash 1 + S_n(\mathbf{1})} \mathtt{R}{+_1} .$$

En utilisant l'opération RÉDUCT, on a $[u, z] \nleftarrow [\sqrt{s'}, \sqrt{q'}]$. Par le Lemme 6.9, on peut déduire

$$[\sqrt{w}, f_a, y, z] \overset{*}{\nleftarrow} N \cdot [\sqrt{q'}]$$

pour un certain $N \in \mathcal{M}_{\Pi(\mathcal{A})}$ tel que $[\![N]\!] = [\![\sqrt{s'}]\!] = s'$. On conclut donc que $\psi(N \cdot [\sqrt{q'}]) = (q', s')$. □

Lemme 7.10. *Soit $M \in \mathcal{M}_{\mathcal{A}}^{\heartsuit}$ et $(q, s) = \psi(M)$. Si $\delta(q, \mathtt{top}(s)) = (f, p_1 \dots p_r)$ pour $p_1 \dots p_r \in Q$, alors il existe $M'_1 \dots M'_r \in \mathcal{M}_{\mathcal{A}}^{\heartsuit}$ tels que pour $1 \leq i \leq r$, $\psi(M'_i) = (p_i, s)$ et $\text{CE}(M)$ est la preuve suivante :*

$$\dfrac{\dfrac{\dfrac{\dfrac{\overline{\qquad} \text{CE}(M'_1) \quad \cdots \quad \overline{\qquad} \text{CE}(M'_r)}{1 \vdash T \qquad\qquad 1 \vdash T} \mathtt{R}\times}{1 \vdash \prod_1^r T} \mathtt{RF}_f}{1 \vdash f} \mathtt{R}{+_f}}{1 \vdash 1 + \coprod_{g \in \Sigma} g} \mathtt{RF}_T}{1 \vdash T} .$$

Démonstration. On commence la preuve de la même façon qu'au 7.9. Par la Proposition 6.5, on peut supposer, sans perte de généralité, que $M = [\sqrt{s}, \sqrt{q}]$. Soit

$a = \mathtt{top}(s)$ et on identifie les sommets de Π_q comme plus haut. Par le même argument qu'au Lemme 7.9, on obtient ceci :

$$[\sqrt{s}, \sqrt{q}] \overset{*}{\leftarrowtail} [\sqrt{w}, f_a, v_a]$$

dont on sait que $[\![\sqrt{w}]\!] \cdot [\![f_a]\!] = s$. Donc $\textsc{ce}(M) = \textsc{ce}([\sqrt{w}, f_a, v_a])$ par définition.

Seulement, cette fois, la preuve $\widetilde{\delta}(q, a)$ a la forme suivante :

$$\dfrac{\dfrac{\dfrac{\dfrac{\sqrt{p_1} : S_n \vdash T \quad \cdots \quad \sqrt{p_r} : S_n \vdash T}{u_3 : S_n \vdash \prod_1^r T}\,\mathtt{R}\times}{u_2 : S_n \vdash f}\,\mathtt{RF}_f}{u_1 : S_n \vdash 1 + \coprod_{g \in \Sigma} g}\,\mathtt{R}+_f}{v_a : S_n \vdash T}\,\mathtt{RF}_T \quad .$$

Puisque $\textsc{Règ}\{v_a, u_1, u_2, u_3\} \subset \mathfrak{R}$, alors l'éliminateur de coupure utilisera l'opération RNext quatre fois consécutives, ce qui produit le segment de preuve recherché. Ensuite, l'éliminateur de coupures poursuit son travail avec r multicoupures en parallèle. Ces multicoupures sont $M'_1 \dots M'_r$ où $M'_i = [r_w, f_a, \sqrt{p_i}]$. Puisque $[\![r_w]\!] \cdot [\![f_a]\!] = s$, alors $\psi(M'_i) = (p_i, s)$. □

À partir des deux lemmes précédents, on peut obtenir le résultat suivant.

Proposition 7.11. *Soit $t = (f, t_1 \dots t_r) \in T$ et $(q, s) \in \mathcal{C}_\mathcal{A}$. S'il existe une exécution $\varrho : T \rightharpoonup \mathcal{C}_\mathcal{A}$ de t à partir de (q, s) et une multicoupure $M \in \mathcal{M}_\mathcal{A}^\heartsuit$ telle que $\psi(M) = (q, s)$, alors $\textsc{ce}(M)$ est bien défini et $\textsc{ce}(M) = \Psi_t$.*

Démonstration. Il suffit de montrer (par induction) que pour tout $h \in \mathbb{N}$, $\textsc{ce}(M)$ et Ψ_t coïncident au moins jusqu'à une hauteur de $4h$. Le cas $h = 0$ étant trivial, soit $h > 0$.

Soit $\varrho(t) = (q_t, s_t)$. Puisque ϱ est une exécution de t à partir de (q, s), alors $(q, s) \twoheadrightarrow_\mathcal{A} (q_t, s_t)$. Par le Lemme 7.9, il existe une multicoupure $M' \in \mathcal{M}_\mathcal{A}^\heartsuit$ telle

que $M \overset{*}{\bowtie} M'$. On a donc $\text{CE}(M) = \text{CE}(M')$, à condition que l'une de ces deux pré-preuves soit bien définie.

Or, puisque ϱ est une exécution, alors $\delta(q_t, \texttt{top}(s_t)) = (f, p_1 \dots p_r)$ pour certains $p_1 \dots p_r \in Q$. Par le Lemme 7.10, $\text{CE}(M')$ et Ψ_t coïncident *au moins* jusqu'à une hauteur de 4. Pour la hauteur restante, on doit vérifier que pour $1 \leq i \leq r$, les multicoupures M_i'' du Lemme 7.10 ont la propriété de coïncider avec Ψ_{t_i} au moins jusqu'à une hauteur de $4(h-1)$. Mais puisque ϱ est une exécution de t_i à partir de (p_i, s_t), cela est vrai par hypothèse d'induction. □

Corollaire (Théorème 7.7)**.** *Soit $\mathcal{A}$ un n-AP qui accepte un Σ-arbre t. Alors*

$$\text{CE}_{\Pi(\mathcal{A})}(\sqrt{\bot}) = \Psi_t.$$

Démonstration. En utilisant FUSION sur $[\sqrt{\bot}]$, on obtient $[\sqrt{\bot}] \bowtie [u, \sqrt{q_0}]$, où $[\![u]\!] = \bot_n$. Donc $\psi([u, \sqrt{q_0}]) = (q_0, \bot_n)$. De plus, t est accepté par $\mathcal{A}$, il y a donc une exécution de t à partir de $(q_0, \bot_n)$. Ainsi, par la Proposition 7.11, on trouve

$$\text{CE}([\sqrt{\bot}]) = \text{CE}([u, \sqrt{q_0}]) = \Psi_t.$$ □

7.4 Un arbre définissable qui n'est pas dans la hiérarchie

L'objectif de cette section est de démontrer que la réciproque du Théorème 7.7, qui dit que tous les arbres circulairement calculables peuvent être situés dans la hiérarchie de Caucal, est fausse. Pour ce faire, on donne un exemple d'un arbre circulairement définissable, donc circulairement calculable par la Proposition 7.1, qui ne se trouve pas dans la hiérarchie.

Rappelons que par des résultats de (Cockett et Santocanale, 2003; Paré et Román, 1989) et le Théorème 4.7, toute fonction primitive récursive $f : \mathbb{N}^K \to \mathbb{N}$ peut être dénotée par une preuve circulaire. C'est le cas, entre autres, des fonctions

primitives récursives à une variable, qu'on peut assimiler à des suites infinies de nombres naturels. Ces derniers sont exprimables par le système dirigé suivant :

$$\mathcal{S} = \left\{ \begin{array}{l} S =_2 N \times S \\ N =_1 1 + N \end{array} \right\}.$$

Or, rappelons (revoir la Figure 7.1) que toute suite infinie $f \in [\![\mathcal{S}]\!]$ peut être représentée par son ***peigne***, $\textsc{Peigne}(f)$, qui est un Σ-arbre, où $\Sigma = \{a, s, 0\}$ avec $\mathrm{ar}(a) = 2$, $\mathrm{ar}(s) = 1$ et $\mathrm{ar}(0) = 0$, défini somme suit (avec le constructeur d'arbres étiquetés de l'Exemple 5 de la Section 2.3) :

$$\begin{aligned} \textsc{Peigne}(n{:}w) &= \mathtt{Cons}(a, [b(n), \textsc{Peigne}(w)]), \qquad \text{où} \\ b(0) &= \mathtt{Cons}(0, []), \\ b(\mathtt{Suc}\ x) &= \mathtt{Cons}(s, [b(x)]). \end{aligned}$$

La fonction $\textsc{Peigne} : [\![S]\!] \to [\![T]\!]$ peut être dénotée par la preuve circulaire de la Figure 7.5, sur le système $\mathcal{S} \cup \mathcal{T}$.

On en conclut que pour toute suite primitive récursive $f \in \mathbb{N}^{\mathbb{N}}$, $\textsc{Peigne}(f) \in \mathbf{CD}$. Pour tout $k \in \mathbb{N}$, soit $h_k : \mathbb{N} \to \mathbb{N}$ la fonction suivante :

$$\begin{aligned} h_0(x) &= x \\ h_{k+1}(x) &= 2^{h_k(x)}, \end{aligned}$$

et posons $f(x) = h_x(1)$. Clairement, f est primitive récursive. On va montrer que $\textsc{Peigne}(f)$ n'est reconnu par aucun n-AP. Il s'agit d'une preuve qui nous fut indiquée par Arnaud Carayol et qui est présente (à peu de choses près) dans sa thèse (Carayol, 2006, Prop. 5.4.3).

Définition. Soit $f, g : \mathbb{N} \to \mathbb{R}$ deux fonctions. On dit que f est ***dominée*** par g s'il existe $x_0 \in \mathbb{N}$ tel que pour tout $x \geq x_0$, on a $f(x) \leq g(x)$. Dans ce cas, on écrit $f \leq g$.

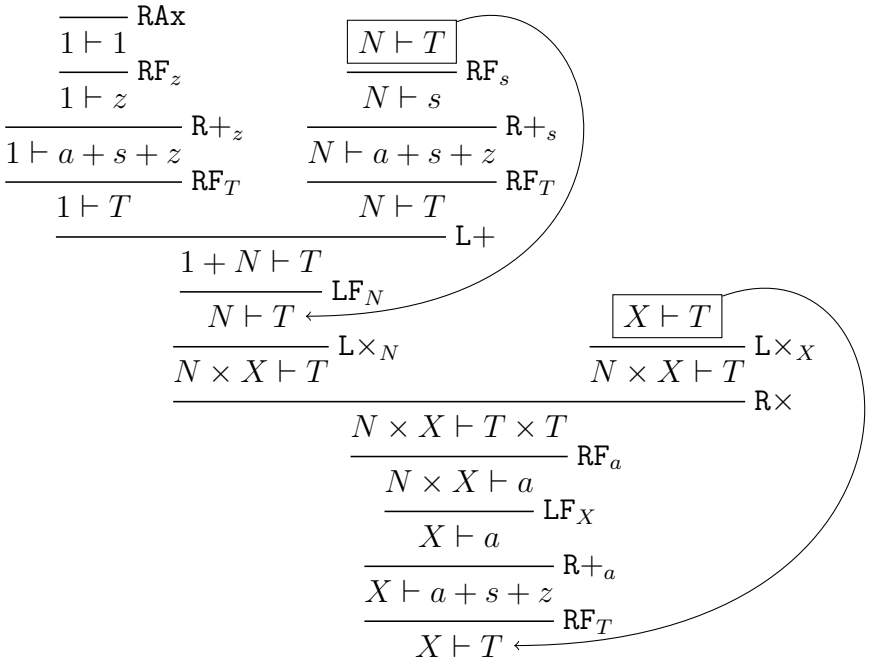


Figure 7.5 Une preuve qui transforme les suites infinies en peignes

Définition. La ***distance*** entre deux langages L_1, L_2 tels que $L_1 \cap L_2 \neq \varnothing$ est définie comme suit :

$$d(L_1, L_2) = \min\{|w| : w \in L_1 \cap L_2\}.$$

Pour $m \in \mathbb{N}$, soit Reg_m l'ensemble des langages réguliers reconnus par un automate à m états. Pour un langage L, son ***indice rationnel*** est la fonction $\rho_L : \mathbb{N} \to \mathbb{N}$ définie par

$$\rho_L(m) = \max\{d(L, R) : R \in \mathrm{Reg}_m, L \cap R \neq \varnothing\}.$$

Lemme 7.12. *Soit $g : \mathbb{N} \to \mathbb{N}$. Si* Peigne$(g)$ *est accepté par un n-AP, alors il existe un polynôme p tel que $g \leq h_{2n} \circ p$.*

Démonstration. Soit $t =$ Peigne(g) et supposons qu'il est accepté par un n-AP.

Alors, par (Knapik *et al.*, 2002, Th. 5.1), t est généré par une *grammaire sûre de niveau n*. Ainsi, par (Caucal, 2003, Th. 3.5), $t \in Term_n$ (tel que défini dans Caucal, 2003) et donc, par (Caucal, 2003, Th. 3.3), t est le *langage arbre* d'un *schéma de niveau n* sur Σ ($t \in n - \mathcal{L}_{\mathrm{OI}}(\Sigma)$), tel que défini dans (Damm, 1982). On peut donc appliquer des résultats de (Damm, 1982) !

Soit $L_t \subseteq \Sigma^*$ le langage des mots formés par les lettres de Σ lues sur les sommets des branches finies de t. Avec $t = \textsc{Peigne}(g)$, on a

$$L_t = \{a^{m+1}s^{g(m)}0 : m \in \mathbb{N}\}.$$

Pour tout $m \in \mathbb{N}$, soit $R_m = a^m s^* z$. Alors $R_m \in \mathrm{Reg}_{m+2}$, et $d(L_t, R_m) = m + g(m-1) + 2$. Donc, pour $m \geq 3$, on a $\rho_{L_t}(m) \geq d(L_t, R_{m-2}) \geq g(m-3)$. Or, par (Damm, 1982, Th. 9.3), ρ_{L_t} est dominé par $h_{2n} \circ p$ pour un certain polynôme p. Il s'ensuit que pour m assez grand, on a $g(m) \leq \rho_{L_t}(m+3) \leq h_{2n}(p(m+3))$. □

En appliquant le Lemme 7.12 à la fonction f définie plus haut, on a $f \leq h^{2n} \circ p$, ce qui est évidemment faux puisque f est une tour d'exponentielles.

CONCLUSION

Résumons les sujets qui furent traités au cours du présent travail. Après avoir introduit quelques outils sur les structures discrètes au Chapitre 1, on a formalisé celles-ci dans un contexte catégorique au Chapitre 2. On est ensuite entré dans le vif du sujet au Chapitre 3 en définissant les preuves circulaires ainsi que plusieurs conditions de garde, toutes équivalentes, devant garantir leur adéquation. Cette adéquation fut démontrée au Chapitre 4 : les preuves circulaires dénotent bel et bien des flèches dans toute catégorie μ-bicomplète. Réciproquement, on a aussi montré que toutes les flèches de la catégorie μ-bicomplète libre étaient la dénotation d'au moins une preuve circulaire. Le point tournant de ce travail, où les preuves circulaires passent d'un outil pour dénoter à un outil pour calculer, se trouve au Chapitre 5, où on a décrit l'algorithme d'élimination des coupures et démontré sa productivité. Ensuite, au Chapitre 6, on a établi la correspondance entre les deux interprétations, algébrique et algorithmique, des preuves circulaires. Enfin, au Chapitre 7, on a montré que l'automate qui opère l'élimination des coupures avait une expressivité strictement supérieure à celle des automates à pile d'ordre supérieur.

Les résultats de la présente recherche revêtent deux saveurs d'intérêt : une saveur théorique et une saveur pratique.

Sur le plan théorique, ils permettent de fonder certains espoirs en la logique *anti-fondée* en présentant un formalisme circulaire épuré au maximum, car propositionnel et sans liberté sur la forme des séquents (on a toujours une seule formule de chaque côté), mais dans lequel tout fonctionne bien, autant du point de vue syn-

taxique que sémantique. Le système a, par ailleurs, l'avantage d'inclure l'induction et la coinduction comme étant les deux faces sémantiques d'une même médaille syntaxique, tout en balisant leur entrelacement par une condition de garde assez permissive. Cela est en contraste avec d'autres formalismes circulaires qui focalisent leur intérêt seulement sur l'induction (Brotherston et Simpson, 2011) ou sur la coinduction (Roşu et Lucanu, 2009). Une avenue de recherche possible serait de tenter d'ajouter au système, par exemple, des règles structurelles (Sambin *et al.*, 2000) ou des opérations de logique modale (Walukiewicz, 2000) ou de logique linéaire (Baelde, 2012), tout en préservant la correspondance avec la sémantique visée ainsi que la propriété d'élimination des coupures.

Sur le plan plus pratique, la condition de garde offre, comme on l'a démontré par le théorème d'élimination des coupures, un critère assez souple pour assurer la productivité d'un programme fonctionnel. Un objectif concret envisageable serait de l'implémenter, par exemple, dans un compilateur Haskell, qui ne vérifierait ainsi plus seulement que les expressions soient bien typées, mais aussi qu'elles soient gardées (il pourrait retourner un avertissement lorsque ce n'est pas le cas).

Par ailleurs, le Chapitre 7 établit des liens effectifs entre deux branches assez éloignées de l'informatique théorique : la théorie des algèbres et coalgèbres, et celle des langages et automates. Ce n'est pas une correspondance exacte, mais des questions demeurent ouvertes qui viseraient à la raffiner.

Par exemple, on a mentionné que la pré-preuve $\Pi(\mathcal{A})$ qui simule un automate $\mathcal{A}$ ne satisfait, en général, pas la condition de garde. Dire qu'elle la satisfait est équivalente à affirmer que pour chaque cycle dans l'automate $\mathcal{A}$, celui-ci traverse une instruction de la forme $(f, p_1 \dots p_r)$. Peut-on le supposer sans perte de généralité ? Si oui, on pourrait conclure que la classe des arbres d'ordre supérieur est contenue dans **CD** et non seulement dans **CC**. Si non, on aurait une forte indication qu'il

y a une différence stricte entre **CD** et **CC**. Ou alors, c'est que notre construction de $\Pi(\mathcal{A})$ n'était pas suffisamment ingénieuse.

Plus généralement, quelle est la différence exacte entre **CD** et **CC**, s'il en est une ? Une analogie avec la théorie du λ-calcul suggère une plus grande expressivité dans **CC**. En effet, la condition de garde jouerait en quelque sorte le rôle du typage des λ-termes : elle nous assure, par le théorème d'élimination des coupures, qu'on ne construit que des fonctions totales. Quand aux preuves non gardées, à l'instar des termes du λ-calcul pur, elles permettent davantage de liberté puisque certaines d'entre elles ne sont pas totales. Par quelle sémantique algébrique peut-on alors décrire **CC** ?

BIBLIOGRAPHIE

Aczel, P. (1988). *Non-well-founded Sets*. Numéro 14 de Lecture Notes. Center for the Study of Language and Information, Stanford University.

Awodey, S. (2006). *Category theory*, volume 49 de *Oxford Logic Guides*. New York : The Clarendon Press Oxford University Press.

Baelde, D. (2012). Least and greatest fixed points in linear logic. *ACM Transactions on Computational Logic*, *13*(1).

Barwise, J. et Moss, L. (1996). *Vicious circles*, volume 60 de *Lecture Notes*. Stanford, Californie : Center for the Study of Language and Information.

Brotherston, J. (2005). Cyclic Proofs for First-Order Logic with Inductive Definitions. Dans B. Beckert (dir.). *Automated Reasoning with Analytic Tableaux and Related Methods : Proceedings of TABLEAUX 2005*, volume 3702 de *LNAI*, 78–92. Springer-Verlag.

Brotherston, J. et Simpson, A. (2011). Sequent calculi for induction and infinite descent. *J. Log. Comput.*, *21*(6), 1177–1216.

Carayol, A. (2006). *Automates infinis, logiques et langages*. (Thèse de doctorat). Université de Rennes 1.

Caucal, D. (2003). On infinite transition graphs having a decidable monadic theory. *Theoretical Computer Science*, *290*(1), 79–115.

Cockett, J. R. B. et Santocanale, L. (2003). Induction, coinduction, and adjoints. *Electronic Notes in Theoretical Computer Science*, *69*, 101–119.

Coquand, T. (1993). Infinite objects in type theory. Dans H. Barendregt et T. Nipkow (dir.). *TYPES*, volume 806 de *Lecture Notes in Computer Science*, 62–78. Springer.

Damm, W. (1982). The IO- and OI-Hierarchies. *Theoretical Computer Science*, *20*(2), 95–207.

David, R., Nour, K. et Raffalli, C. (2004). *Introduction à la logique* (2e éd.). Dunod.

Eilenberg, S. et MacLane, S. (1945). General theory of natural equivalences. *Transactions of the American Mathematical Society*, *58*(2), 231–294.

Fortier, J. (2015). Higher-Order Pushdown Trees are Circularly Computable. Dans D. Baelde et J. Alglave (dir.). *Vingt-sixièmes Journées Francophones des Langages Applicatifs (JFLA 2015)*, Le Val d'Ajol, France. Disponible à `https://hal.inria.fr/hal-01099127`.

Fortier, J. et Santocanale, L. (2013). Cuts for circular proofs : semantics and cut-elimination. Dans S. R. D. Rocca (dir.). *CSL*, volume 23 de *LIPIcs*, 248–262. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

Fortier, J. et Santocanale, L. (2014). Cuts for circular proofs. Dans N. Galatos, A. Kurz, et C. Tsinakis (dir.). *TACL 2013*, volume 25 de *EPiC Series*, 72–75. EasyChair.

Gentzen, G. (1935). Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, *39*(1), 176–210, 405–431.

Girard, J. (2006). *Le point aveugle : cours de logique. Vers la perfection*. Visions des sciences. Hermann.

Gödel, K. (1931). Über Formal Unentscheidbare Sätze der Principia Mathematica Und Verwandter Systeme I. *Monatshefte für Mathematik*, *38*(1), 173–198.

Jacobs, B. et Rutten, J. (1997). A tutorial on (co)algebras and (co)induction. *EATCS Bulletin*, *62*, 62–222.

Joyal, A. (1995). Free bicomplete categories. *Comptes rendus mathématiques de l'Académie des Sciences du Canada*, *XVII*(5), 219–224.

Joyal, A. (1997). Free lattices, communication and money games. Dans M. L. D. Chiara, K. Doets, D. Mundici, et J. van Benthem (dir.). *Logic and Scientific Methods : Volume One of the Tenth International Congress of Logic, Methodology and Philosophy of Science, Florence, August 1995*, volume 259 de *Synthese Library*, 29–68., Dordrecht. Springer.

Kőnig, D. (1936). *Theorie der endlichen und unendlichen Graphen.* Leipzig : Akademische Verlagsgesellschaft.

Knapik, T., Niwiński, D. et Urzyczyn, P. (2002). Higher-order pushdown trees are easy. Dans Nielsen et Engberg (2002), 205–222.

Kozen, D. (1983). Results on the propositional μ-calculus. *Theoretical Computer Science*, *27*(3), 333–354.

Lambek, J. (1968). A fixpoint theorem for complete categories. *Mathematische Zeitschrift*, *103*, 151–161.

Lambek, J. et Scott, P. J. (1988). *Introduction to higher order categorical logic.* New York, NY, USA : Cambridge University Press.

Lawvere, F. (1969). Diagonal arguments and cartesian closed categories. Dans *Category Theory, Homology Theory and their Applications II*, volume 92 de *Lecture Notes in Mathematics*, 134–145. Springer Berlin Heidelberg.

Mac Lane, S. (1998). *Categories for the working mathematician* (2e éd.). New York : Springer-Verlag.

Nielsen, M. et Engberg, U. (dir.) (2002). *Foundations of Software Science and Computation Structures, 5th International Conference, FOSSACS 2002*, volume 2303 de *Lecture Notes in Computer Science*. Springer.

Paré, R. et Román, L. (1989). Monoidal categories with natural numbers object. *Studia Logica*, *48*(3), 361–376. http://dx.doi.org/10.1007/BF00370829

Perrin, D. et Pin, J.-E. (2004). *Infinite Words, Automata, Semigroups, Logic and Games*, volume 141. Elsevier.

Pratt, V. R. (1981). A decidable mu-calculus : Preliminary report. Dans *Proceedings of the 22Nd Annual Symposium on Foundations of Computer Science*, SFCS '81, 421–427., Washington, DC, USA. IEEE Computer Society.

Roşu, G. et Lucanu, D. (2009). Circular coinduction : A proof theoretical foundation. In A. Kurz, M. Lenisa, et A. Tarlecki (dir.), *Algebra and Coalgebra in Computer Science*, volume 5728 de *Lecture Notes in Computer Science* 127–144. Springer Berlin Heidelberg.

Russell, B. (1908). Mathematical Logic as Based on the Theory of Types. *American Journal of Mathematics*, *30*(3), 222–262.

Sambin, G., Battilotti, G. et Faggian, C. (2000). Basic logic : Reflection, symmetry, visibility. *Journal of Symbolic Logic*, *65*(3), 979–1013.

Santocanale, L. (2000). *Sur les μ-treillis libres*. (Thèse de doctorat). Université du Québec à Montréal.

Santocanale, L. (2001). *A Calculus of Circular Proofs and its Categorical Semantics*. Rapport technique RS-01-15, BRICS, daimi. 30 pp.

Santocanale, L. (2002a). A calculus of circular proofs and its categorical semantics. Dans Nielsen et Engberg (2002), 357–371.

Santocanale, L. (2002b). μ-bicomplete categories and parity games. *Theoretical Informatics and Applications*, *36*, 195–227.

Sprenger, C. et Dam, M. (2003). On the Structure of Inductive Reasoning : Circular and Tree-shaped Proofs in the μ-Calculus. Dans A. D. Gordon (dir.). *Proceedings of FOSSACS'03*, volume 2620, 425–440. Springer-Verlag.

Walukiewicz, I. (2000). Completeness of Kozen's Axiomatisation of the Propositional μ-Calculus. *Information and Computation*, *157*(1-2), 142–182.

Whitehead, A. N. et Russell, B. (1910-1913). *Principia Mathematica*. Cambridge University Press.

Yanofsky, N. S. (2003). A universal approach to self-referential paradoxes, incompleteness and fixed points. *Bulletin of Symbolic Logic*, *09*(3), 362– 386.